WELCOME TO THE OLIVIA WEB TOOL!

USER GUIDE

Dear SMEs, data protection officers, and valued users of the **Olivia web tool**,

This guide provides a comprehensive overview of the Olivia web tool, its purpose, and instructions for use.

What is the Olivia Web Tool?

The Olivia web tool is the main outcome of the ARC2 project, designed specifically for micro, small, and medium-sized enterprises.

This initiative is co-founded by the European Union and implemented through a collaborative partnership involving:

- Croatian Data Protection Authority (AZOP)
- Italian Data Protection Authority (Garante Privacy)
- Faculty of Organization and Informatics, Varaždin
- Vrije University, Brussels
- University of Florence

We developed Olivia to simplify your understanding of data protection legislation, clarify your obligations under the General Data Protection Regulation (GDPR), and streamline the compliance process.

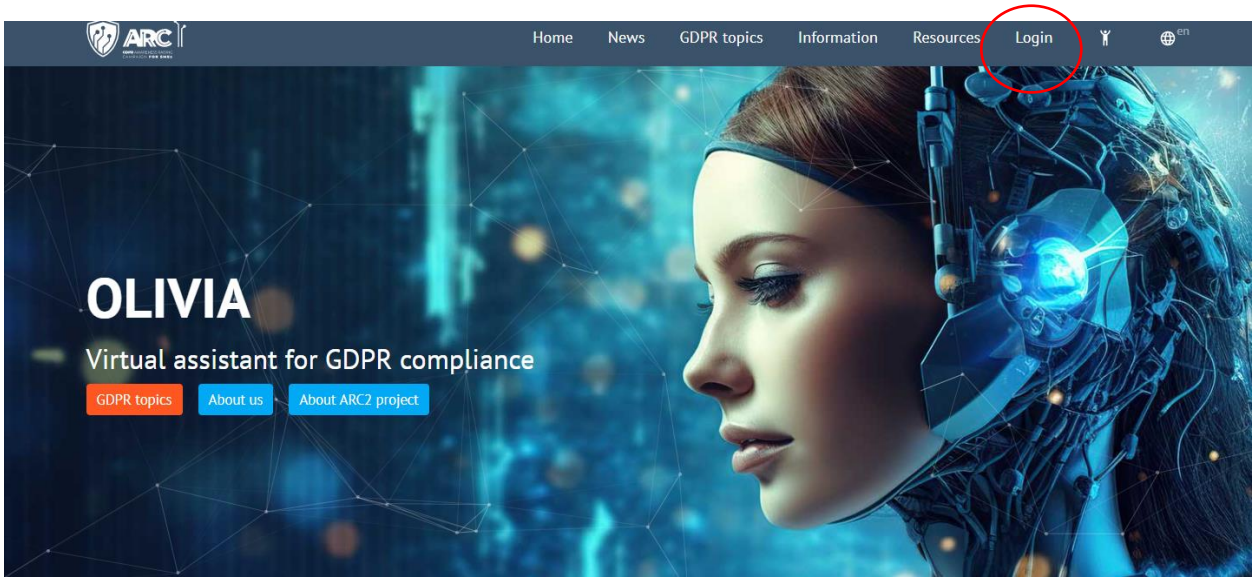
Getting Started to begin using Olivia, please follow these steps:

1. Navigate to the top of the page
2. Locate the "LOGIN" button in the navigation bar
3. Click on "LOGIN" to access the registration page
4. Complete the registration process to create your account

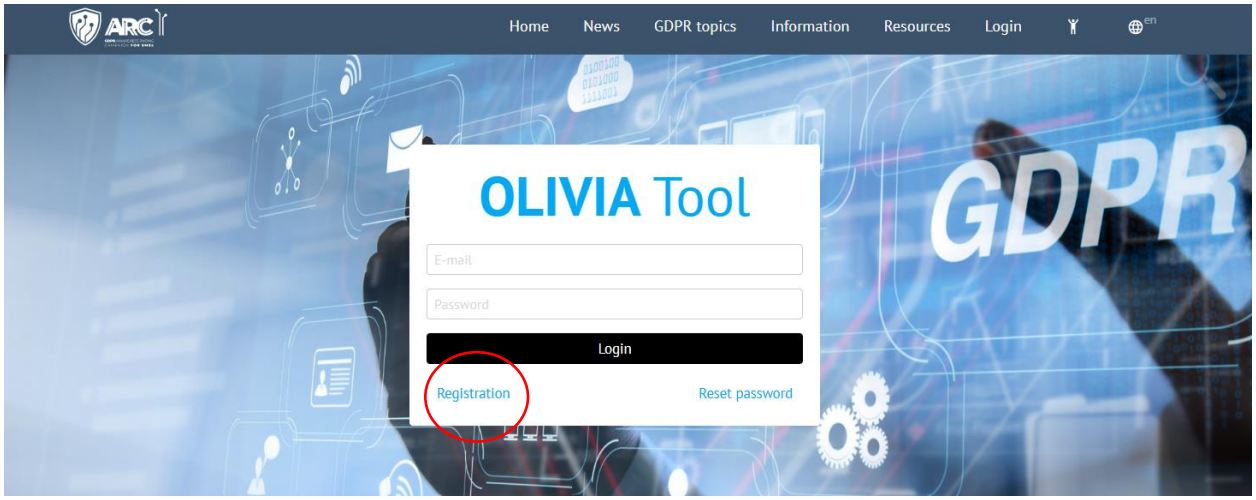
Once registered, you'll have full access to Olivia's features and resources, empowering you to enhance your data protection practices.

We're excited to assist you on your journey towards GDPR compliance!

REGISTRATION



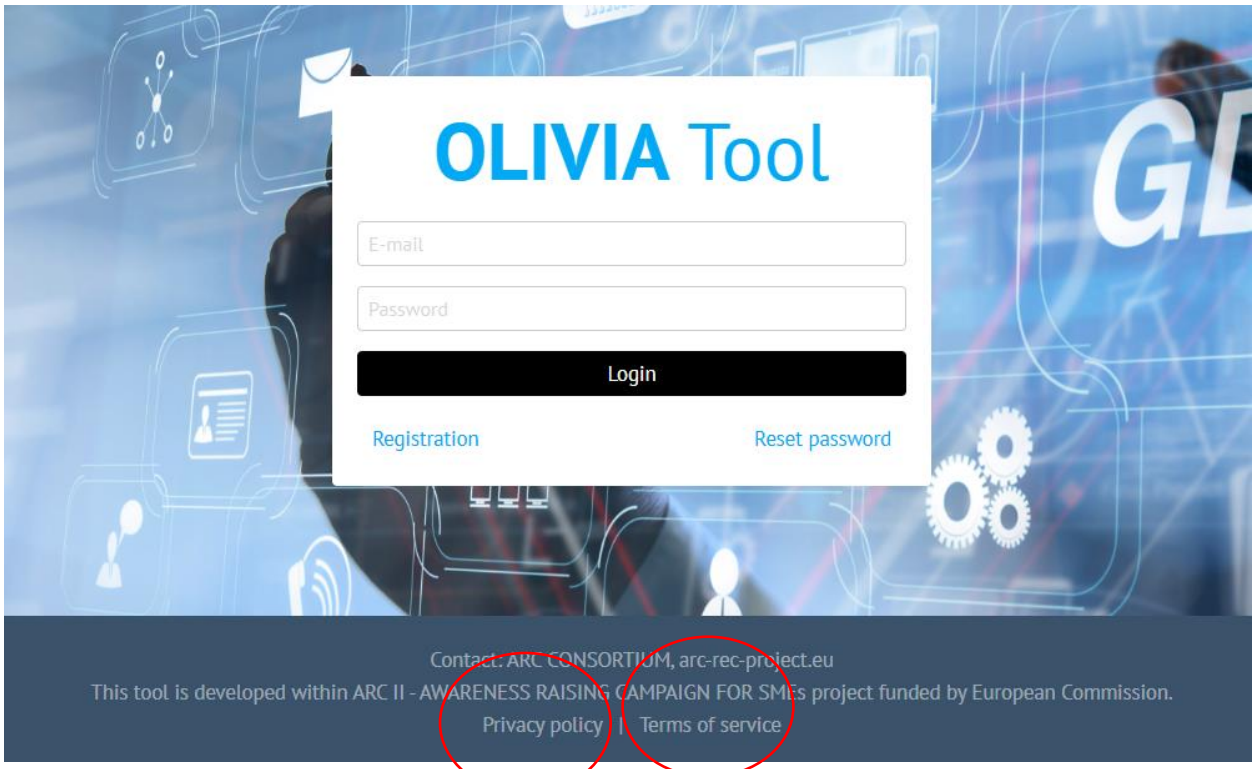
CLICK ON "REGISTRATION"



INSERT YOUR NAME, LAST NAME, E-MAIL, PASSWORD, CONFIRM YOUR PASSWORD.

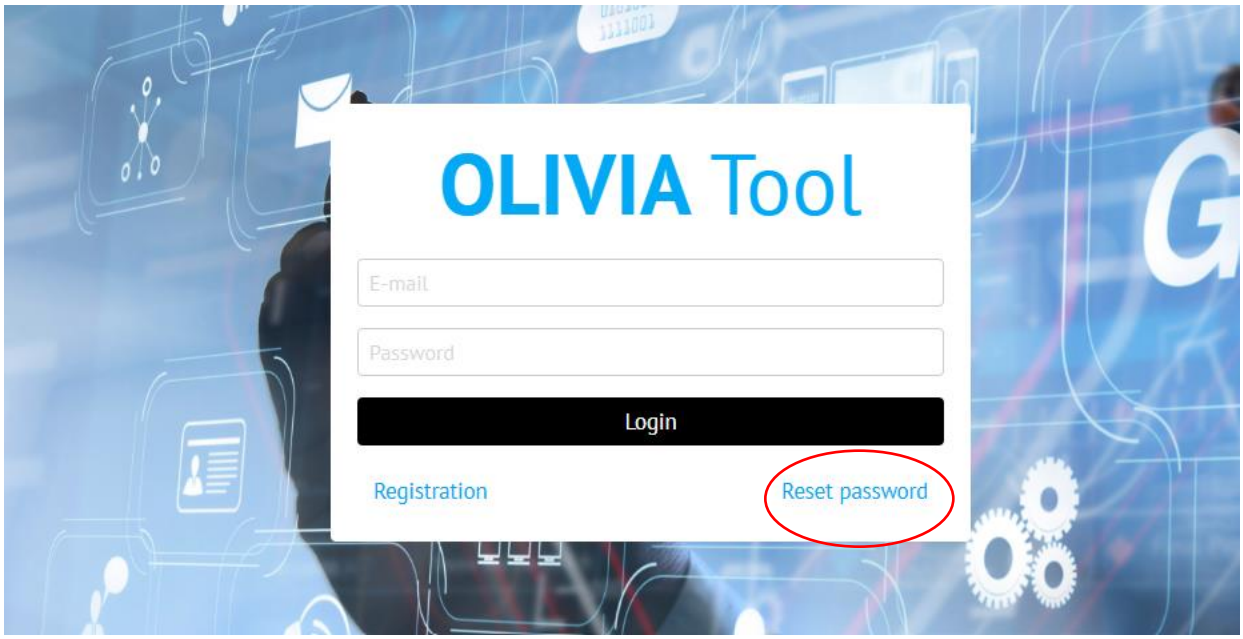
BEFORE REGISTRATION READ THE TERMS AND CONDITIONS OF SERVICES THAT WE ARE PROVIDING: https://olivia-gdpr-arc.eu/italian/it/gdpr/terms-of-service/active

TO REGISTER AND USE OLIVIA, YOU NEED TO ACCEPT THE TERMS AND CONDITIONS OF SERVICE. BEFORE ACCEPTING THE TERMS OF SERVICE, READ THE PRIVACY POLICY CAREFULLY.



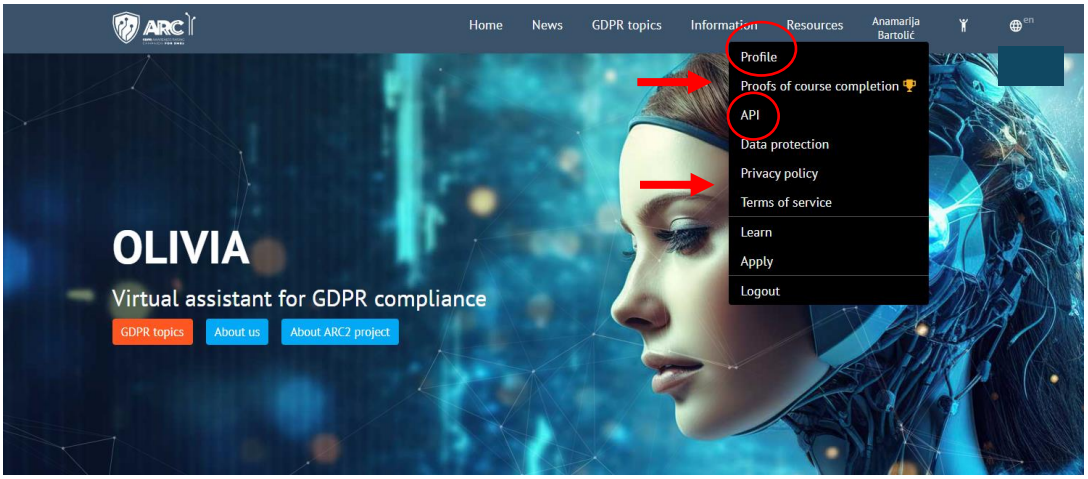
After completing the registration process, you will receive a confirmation notice at the email address you provided. To activate your OLIVIA account and start using it, simply click on the activation link included in the email. Once activated, you'll have full access to all the features and resources OLIVIA offers to assist you with GDPR compliance.

IF YOU WANT TO RESET THE PASSWORD, YOU NEED A CLICK **“RESET”**



After requesting a password change, you will receive an email containing instructions:

1. Check your inbox for an email from our system
2. The subject line will indicate it's about password reset
3. Open the email and locate the password reset link
4. Click on the link to be directed to a secure page
5. On this page, you'll be able to create and confirm your new password



PROFILE Section: In the PROFILE section, you can click on the **"Modify your password"** button to change your password. You can also update your first and last name. Please note that you cannot change your email address.

PROOFS OF COURSE COMPLETION Section: In the PROOFS OF COMPLETION section, you will find certificates for all courses you have successfully completed.

Data Protection Section: The Data Protection section provides information on how to exercise your rights under the General Data Protection Regulation (GDPR).

Application Programming Interface (API) Section: The Application Programming Interface (API) section offers a list of available API endpoints accessible to each user. The API only allows for reading/retrieving data. Each listed API endpoint contains: its name; URL; a short description; a cURL example

After successfully registering with OLIVIA, you can begin your journey towards GDPR compliance, which we are confident will be smoother with OLIVIA's assistance. 😊

OLIVIA is an e-learning platform comprising 15 courses (GDPR TOPICS), each consisting of theoretical and practical modules. These 15 courses cover:

• Explanations of all your obligations as a data controller or data processor

• Educational materials and videos

• Knowledge tests

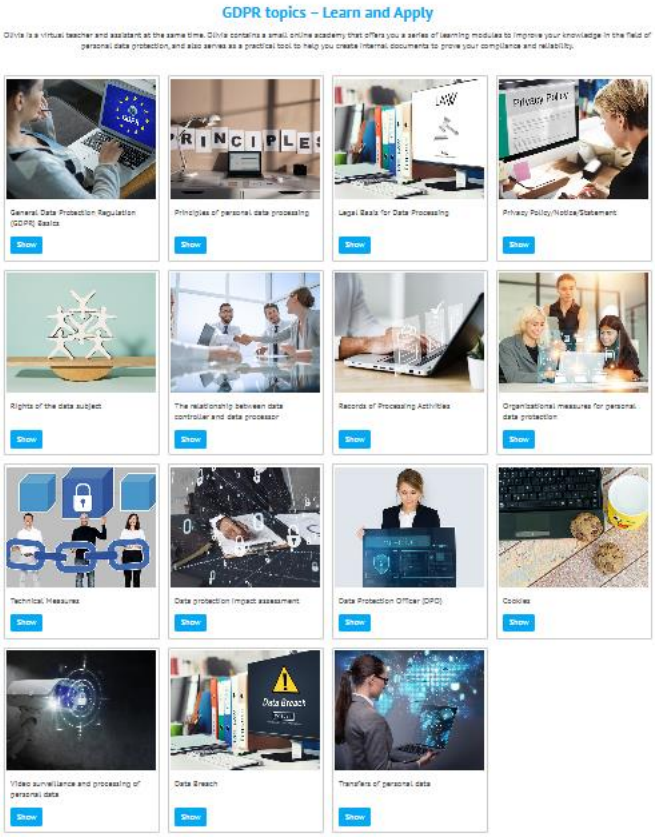
• Webinars

• Presentations

• Templates for creating documents to demonstrate your GDPR compliance

This comprehensive approach ensures that you not only understand the GDPR requirements but also have the practical tools to implement them in your organization. Whether you're new to data protection or looking to refine your existing practices, OLIVIA provides the resources you need to navigate the complexities of GDPR compliance effectively.

Each theoretical part consists of short lessons and a brief educational video. The learning process involves watching the educational video and studying all the lessons thoroughly. After completing these steps, you'll be able to take the knowledge test. A passing score for the test is 80% or higher. If you achieve a score of 80% or above, Olivia will automatically generate a certificate. This certificate confirms your successful completion of the theoretical module. This structured approach ensures a comprehensive understanding of each topic before moving on to practical applications, reinforcing your knowledge of GDPR principles and requirements.



We recommend starting with the **first course, "General Data Protection Regulation Basics,"** to familiarize yourself with the fundamental concepts and essential steps every organization needs to take when complying with the General Data Protection Regulation.

After mastering the basic terminology in the first course, we suggest proceeding in order from **the 2nd to the 15th course: principles of personal data processing, lawful bases for personal data processing, privacy policy, data subject rights, relationship between controller and processor, records of personal data processing activities, organizational and technical measures, data protection impact assessment, data protection officer, processing of personal data through cookies, video surveillance, processing of biometric data and tracking of workers via GPS, personal data breaches, and transfers to third countries.**

We emphasize that the following courses are applicable to all organizations, as they cover GDPR obligations relevant to all data controllers: principles of personal data processing, lawful basis, privacy policy, data subject rights, and organizational and technical measures. Any organization processing personal data must comply with the principles for personal data processing referred to in Article 5,

determine the appropriate legal basis for processing personal data in accordance with Article 6, inform data subjects about the processing of their personal data pursuant to Articles 13 and 14, respect data subjects' rights, and implement appropriate organizational and technical measures to protect personal data.

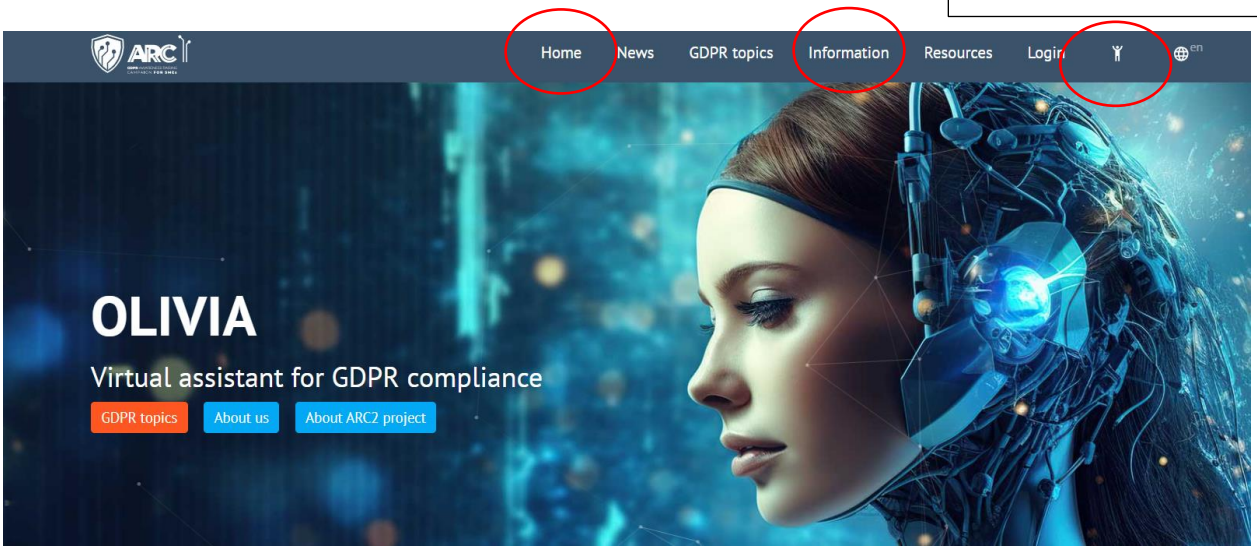
Regarding the other courses, it's important to note that not every organization is obliged to carry out a Data Protection Impact Assessment (DPIA) or appoint a Data Protection Officer (DPO). Additionally, not all data controllers work engages data processors.

Furthermore, courses relating to video surveillance, processing biometric data and processing of personal data via GPS will be useful to controllers carrying out such processing activities, and not to all controllers. The same applies to courses on the processing of personal data through cookies and transfers of personal data to third countries.

OLIVIA also contains webinars and presentations on various data protection topics (available only in Croatian and Italian). If you want to deepen your knowledge on a special topic, this is the section for you!

All webinars and presentations will remain available permanently and free of charge, and the main advantage is that you can view them at a time that suits you.

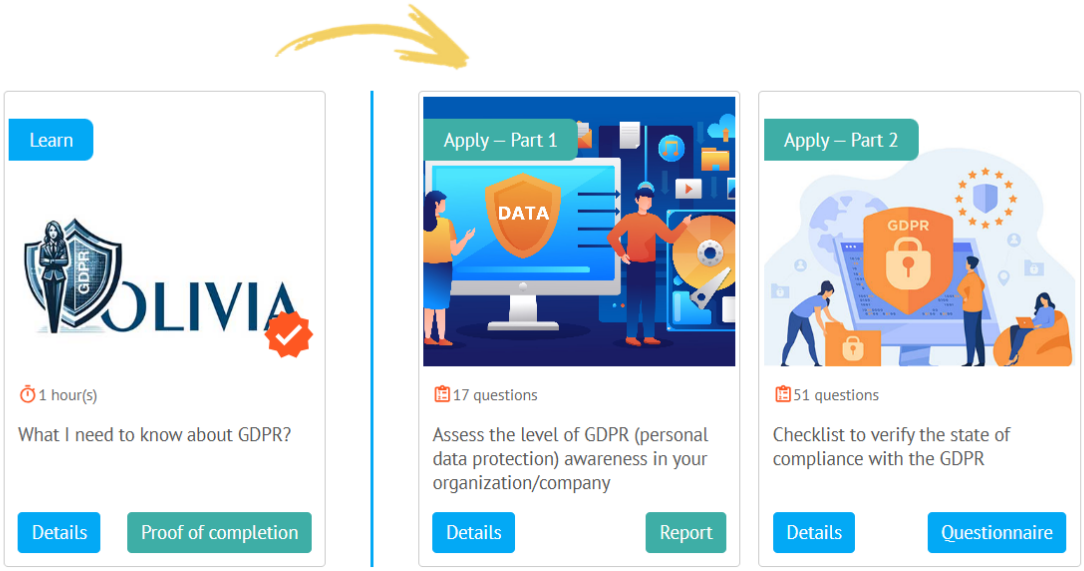
Special features for users with disabilities



In the section **INFORMATION,** you can find more information about the project we are implementing with the aim of facilitating compliance with GDPR primarily to micro, small, medium-sized enterprises and craftsmen. In the **NEWS** section, we will publish information about our activities and interesting facts from the world of personal data protection. Also, the NEW section contains the most relevant judgments of the Court of Justice of the EU in the field of personal data protection for the period 2020-2023.

The following is a short guide through 15 courses that **Olivia** contains, to make this journey towards GDPR compliance as simple and enjoyable as possible.

1. General Data Protection Regulation (GDPR) Basics

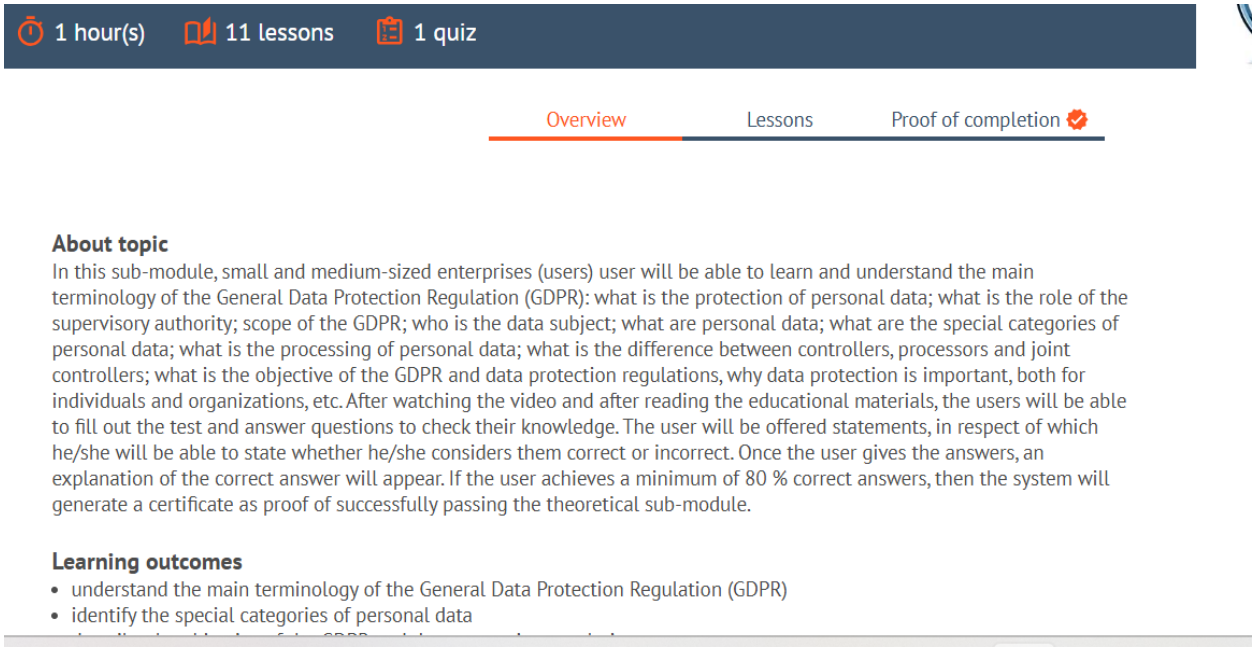


In the theoretical module of the course **"GDPR Basics",** users of the Olivia web tool have the opportunity to learn:

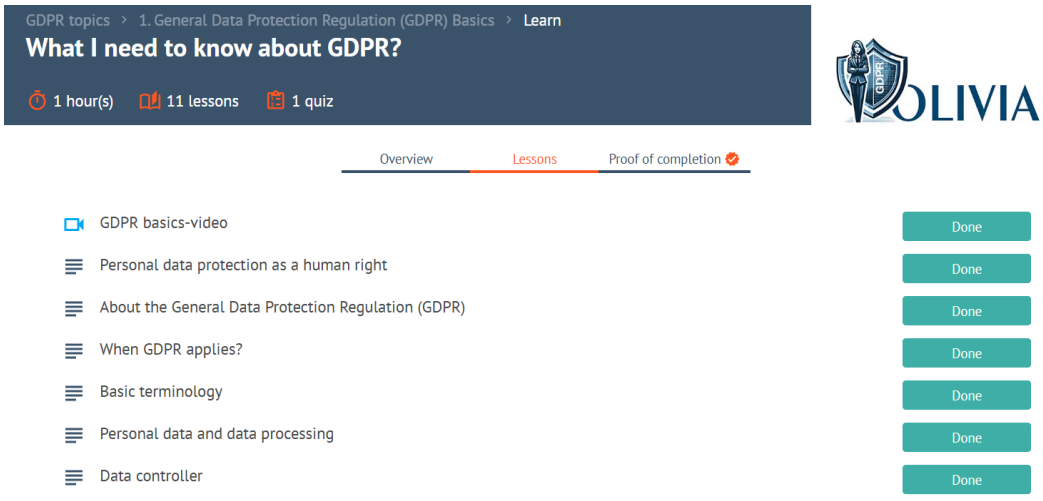
- basic terminology of the General Data Protection Regulation;
- the legislative framework in the Republic of Croatia and Italy
- what is the right to personal data protection;
- the scope of the General Data Protection Regulation;
- what is the objective of the GDPR and data protection legislation in general;
- what is the role of the supervisory authority;
- who the data subjects are;
- what the personal data are and what the special categories of personal data are;
- what is the processing of personal data;
- the distinction between controllers, processors and joint controllers;
- why the protection of personal data is important for both individuals and organisations

The aim of this module is to help users master the basics of the GDPR and understand what are the key steps to comply with the GDPR.

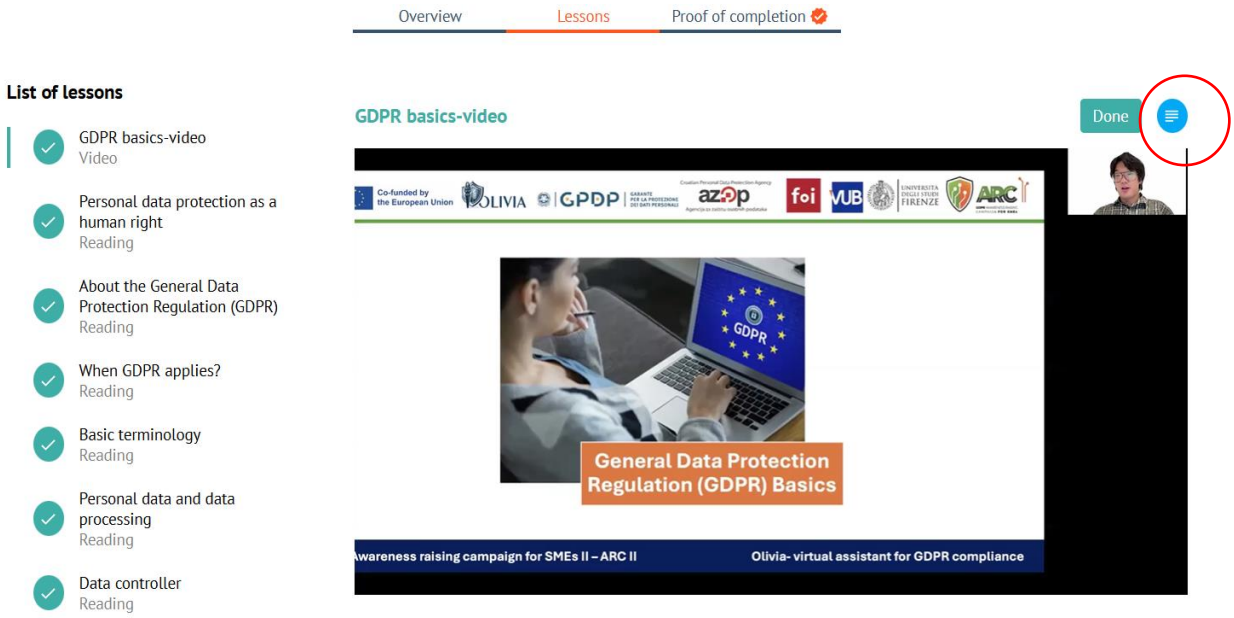
When you open the GDPR basics course, you can find basic information about the course topic in the **OVERVIEW** section.



In the section LESSONS, there are lessons you need to master and a short educational video that will make it easier for you to understand the topic. Once you have mastered all the lessons and watched the educational video, you can mark the video and lessons with **DONE.**

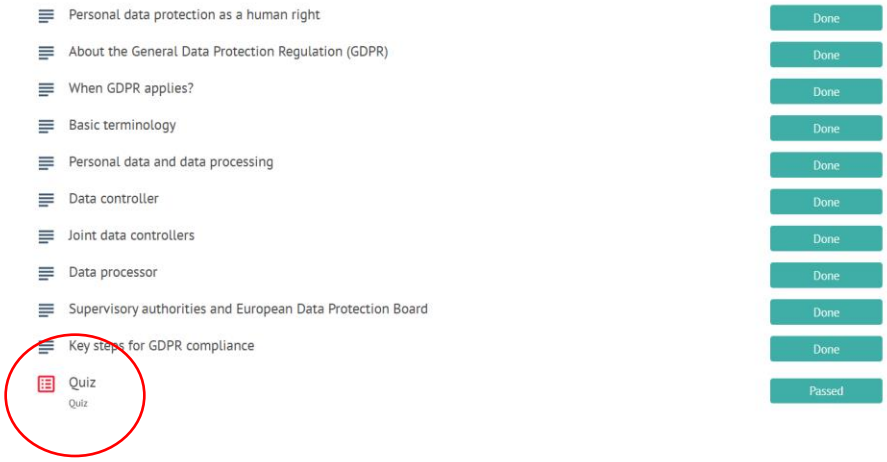


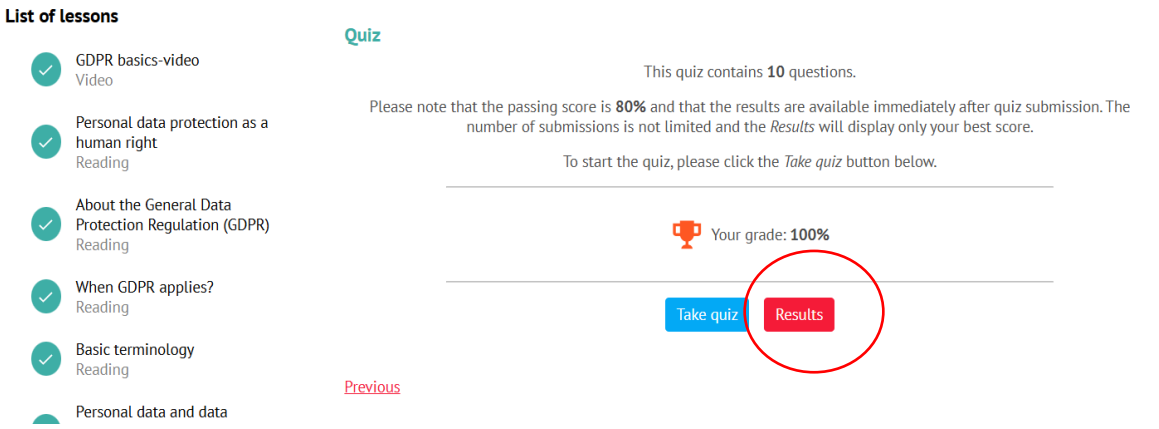
After watching the short educational video, there are 10 lessons that need to be studied in detail to be able to pass the test.



For each lesson in the theoretical part, you have the option to click on the icon marked in red and add your notes related to a specific topic.

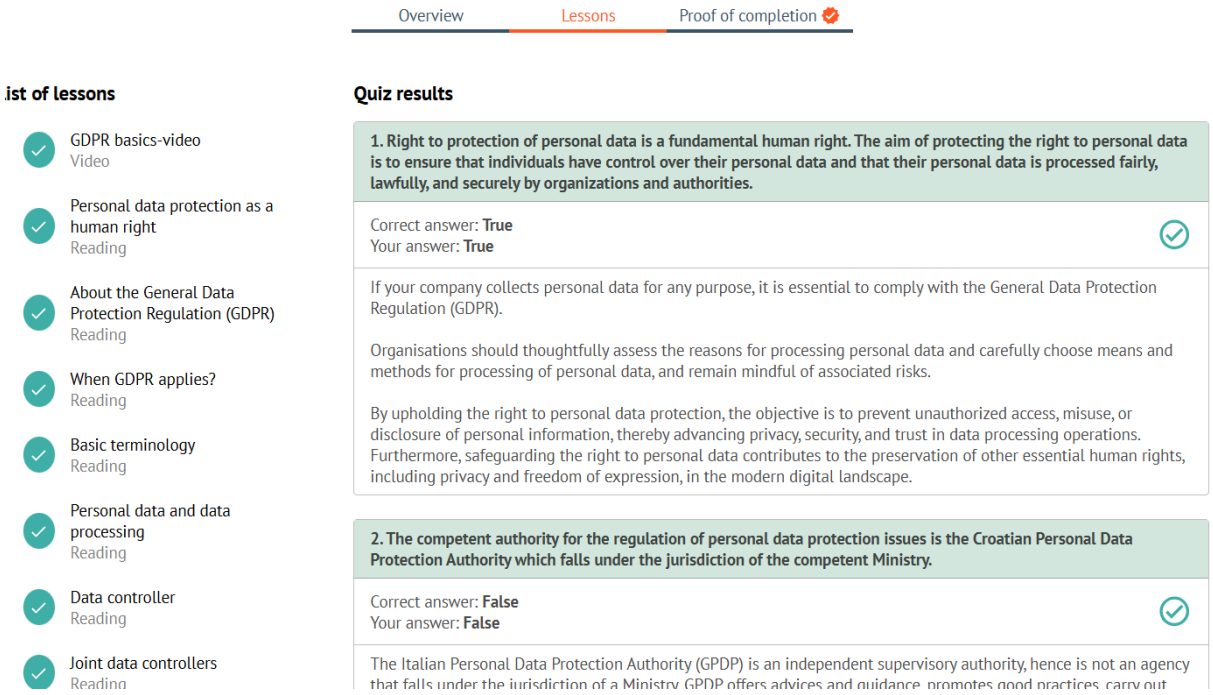
KNOWLEDGE TEST (QUIZ)



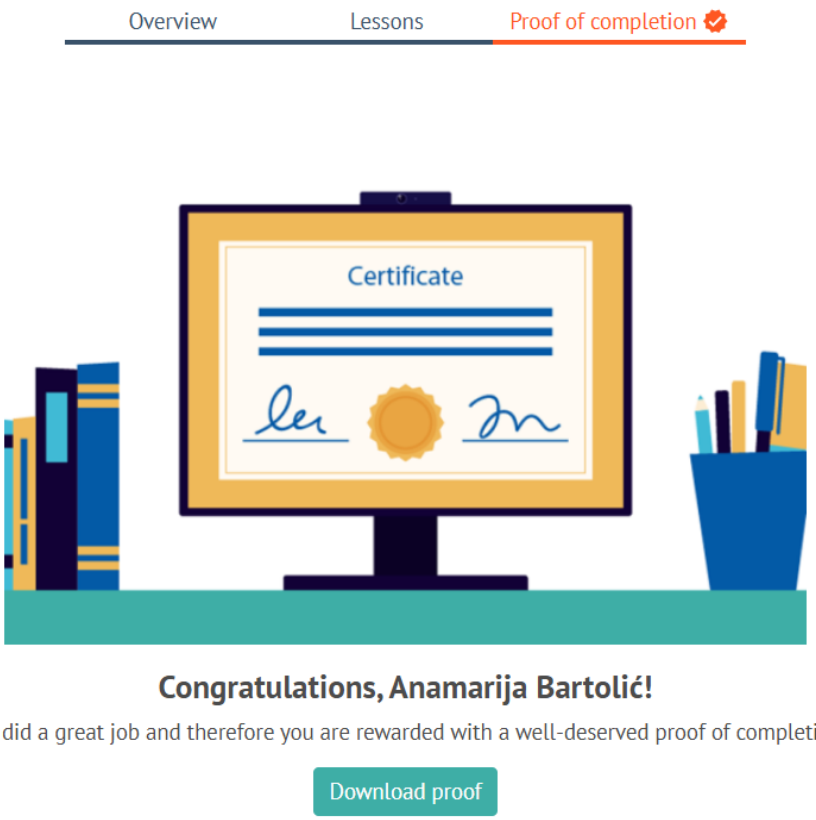


If you have more than 80% correct answers, Olivia will generate confirmation of successful completion of the module.

By clicking on the RESULTS button, a page opens where you can see your answers and explanations.



When you click on the "PROOF OF COMPLETION", the page where you can download your confirmation will open. This proof of completion can be used as one of the organisational measures and as a tool to educate and motivate employees to learn about personal data protection. In this way, you are working actively to raise awareness on personal data protection within your organisation.



The practical part of the "GDPR Basics" course consists of two online forms (self-assessment questionnaires):

- Self-assessment questionnaire on the level of personal data protection in a company (organisation)

When you open the practical module, on the webpage you will see three sections: **Overview, Questionnaire, Report**. Under **OVERVIEW** you can find some basic information about the QUESTIONNAIRE.

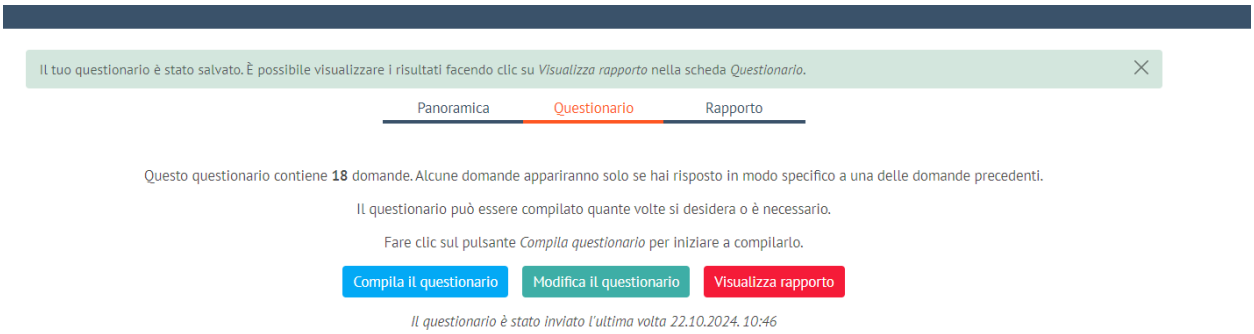
CHOOSE QUESTIONNAIRE

In this practical module, you will be asked for essential information about data processing in your organization, i.e. the following information: whether you process personal data of customers, employees; whether they process data on sex, religion, health or other types of sensitive data; whether you use the personal data that you collect and store for specific, explicit and legitimate purposes; if you keep personal data only for as long as necessary for the purposes for which the personal data are processed, etc. Furthermore, users will be able to answer questions to determine whether they are data controllers, processors or joint controllers.

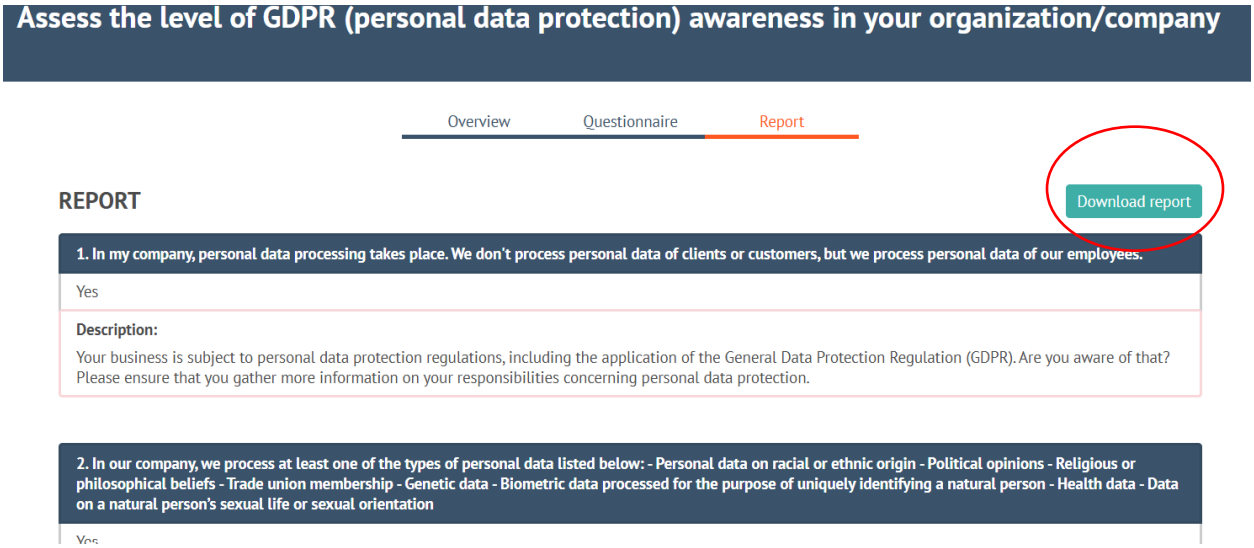
It is essential that you identify the role your organisation/company plays in data processing activities, as organisations/companies can also play all three roles at the same time.

For example, a marketing agency is at the same time a data controller for some processing activities and together with an air transport company is a joint controller and data processor for other organisations that have engaged them to carry out marketing activities.

After answering the 17 questions in the questionnaire, Olivia will generate an explanatory report regarding your obligations under the General Data Protection Regulation.



REPORT CAN BE DOWNLOADED IN .PDF FORMAT IN SECTION DOWNLOAD REPORT.



- GDPR Self-Assessment Questionnaire

We strongly recommend that all organizations processing personal data complete the GDPR self-assessment questionnaire. This comprehensive tool is designed to help you evaluate your current data protection practices, identify potential gaps in compliance, and guide you towards full adherence to GDPR requirements.**The questionnaire consists of 51 questions.**

Questions from the questionnaire will help organizations to map the personal data they are currently processing, identify the legal basis for the collection (processing) of personal data and the period storage for each category of data.

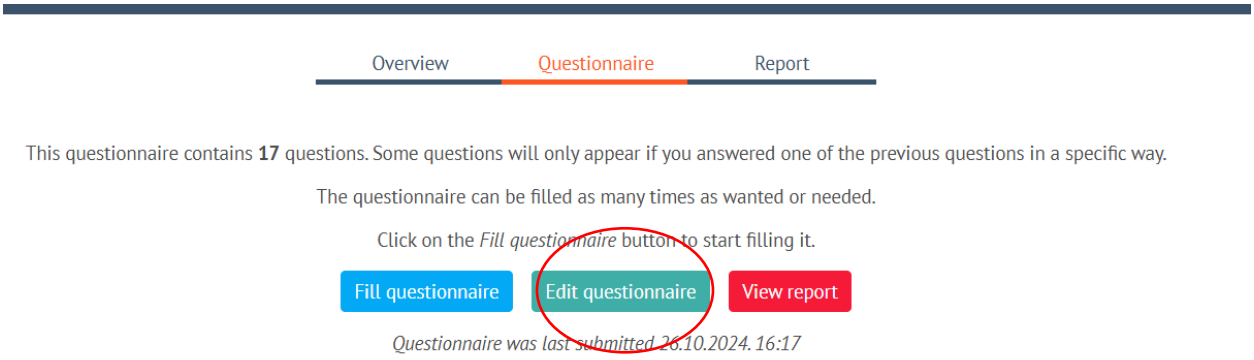
Conducting this exercise will help identify where urgent corrective actions are needed to achieve compliance with the General Data Protection Regulation.

This GDPR compliance self-assessment questionnaire contains more detailed questions in the following areas:

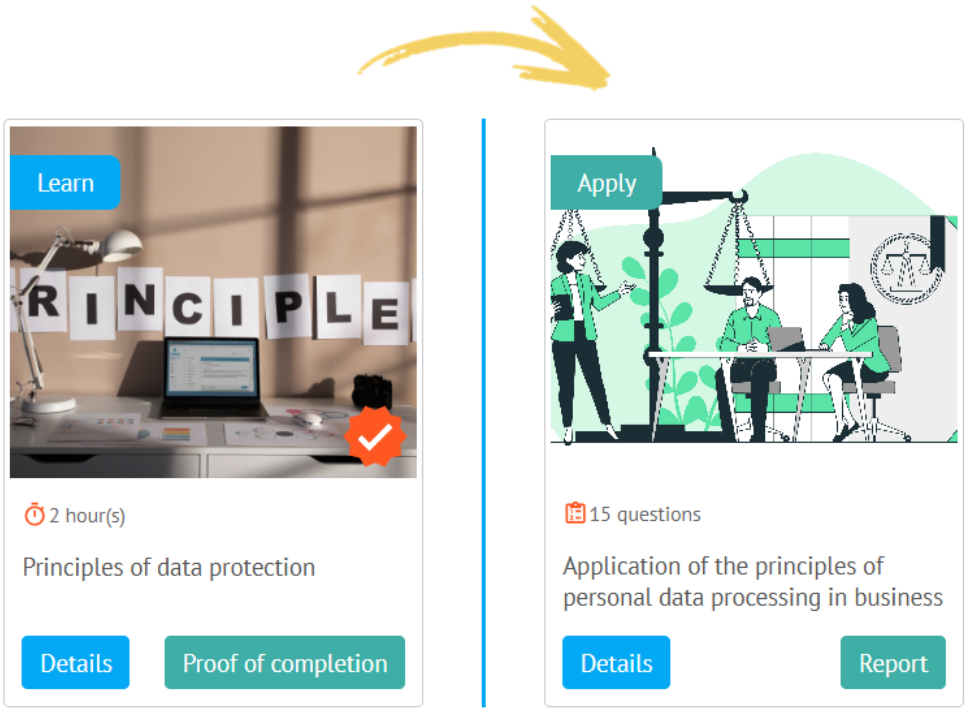
- **personal data processed by the organisation;**
- **legal bases for the processing of personal data;**
- **principles relating to processing of personal data;**
- **informing the data subject about the processing of his or her personal data;**
- **risk assessment;**
- **data security;**
- **data breaches;**
- **international data transfers.**

Your responses to the questionnaire can be saved and modified at any time. There is no limit to how many times you can complete or revise the questionnaire.

After you have completed the questionnaire, in the section **VIEW REPORT,** you can download the results/report in pdf. format. You can fill out the questionnaire an unlimited number of times. If you wish to modify the content of the questionnaire, please choose **EDIT QUESTIONNAIRE.**



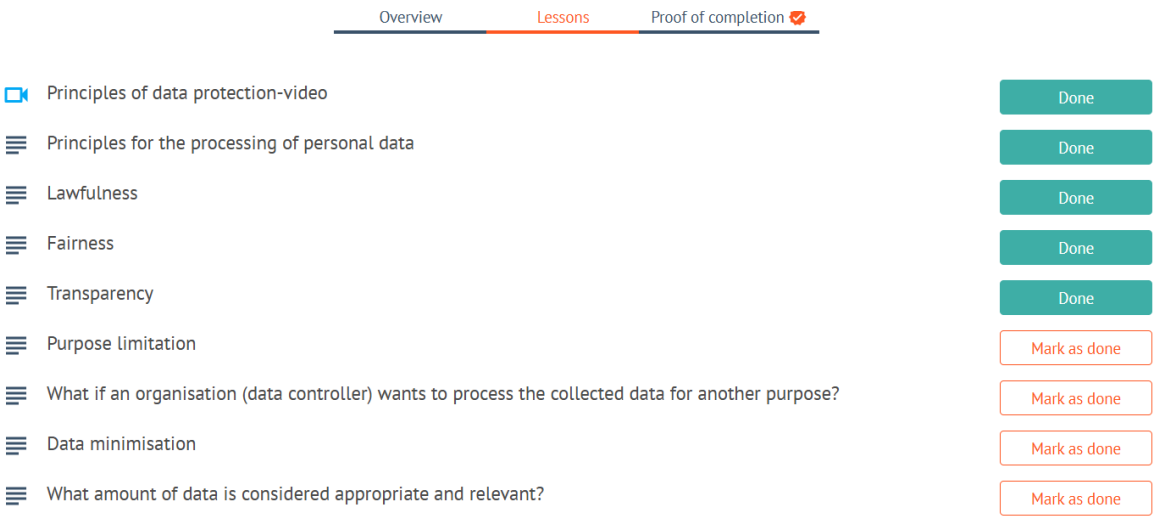
2. Principles relating to processing of personal data



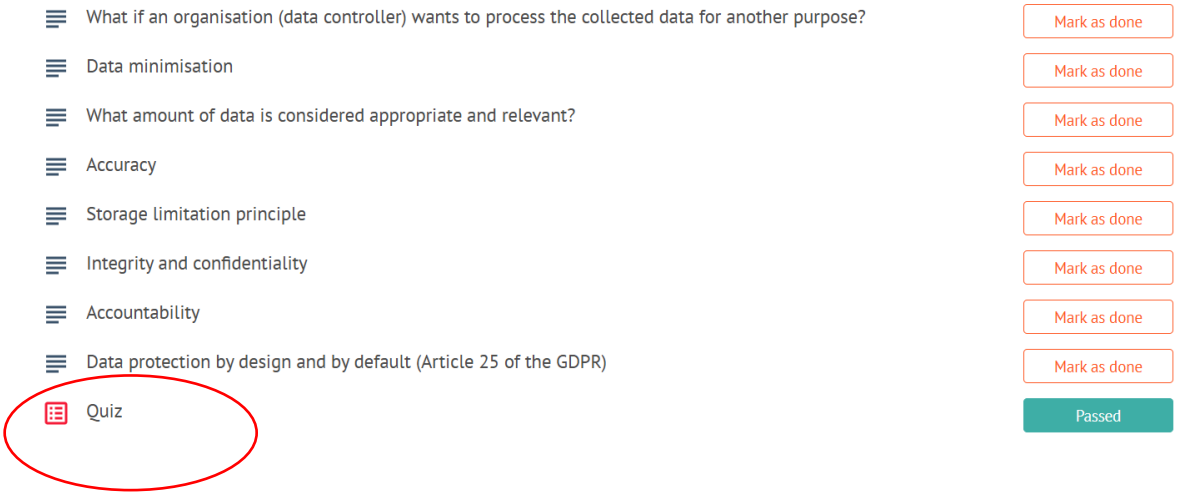
In the theoretical module of the course "Principles relating to processing of personal data", users of the Olivia web tool have the opportunity to learn:

- what principles of personal data processing are prescribed by the GDPR
- how to comply with the principles outlined in article 5 of the GDPR; starting with lawfulness, fairness and transparency
- how to comply with the principle of purpose limitation and what to do if they want to process personal data for a different purpose than the one for which they initially collected the data
- what undertakings (controllers) need to do to comply with the principle of data minimisation and what amount of data is considered adequate and relevant
- why the principle of accuracy is important and how to comply with it
- what is the principle of storage limitation and how to determine the retention period of personal data
- why the principle of integrity and confidentiality is important and what measures should be taken to comply with that principle;
- what is the principle of accountability and how to demonstrate compliance with the GDPR
- what is data protection by design and by default and how to apply it in practice

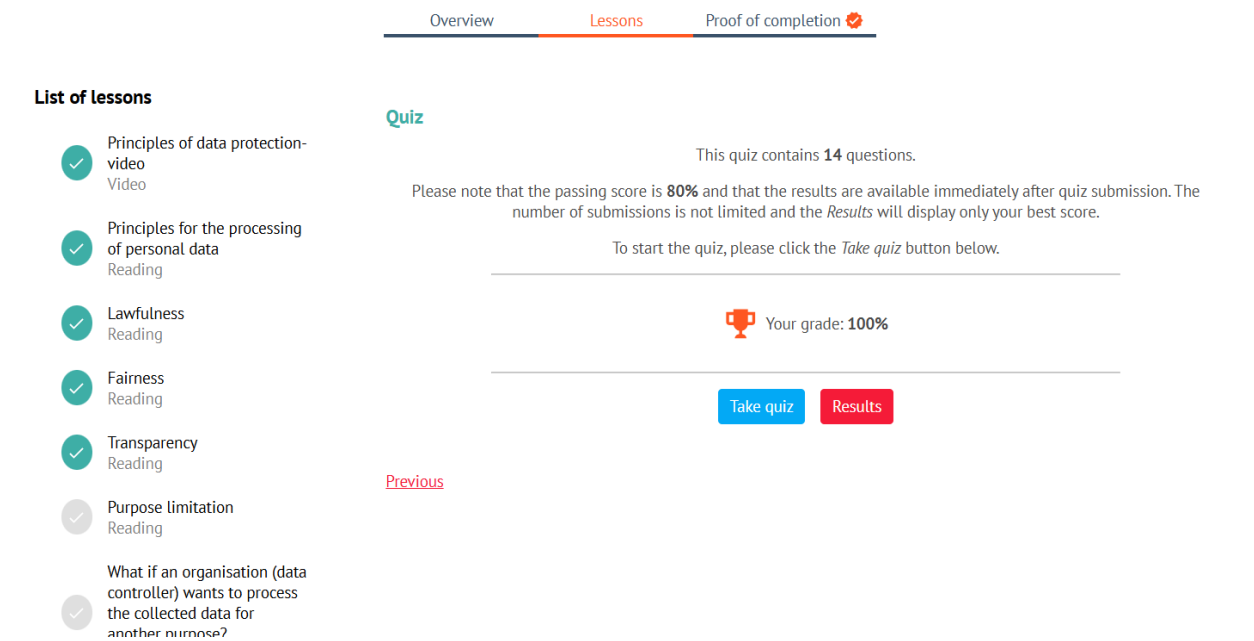
The aim of this theoretical module is to introduce users to the importance of understanding the principles of personal data processing referred to in Article 5 of the GDPR through practical examples.

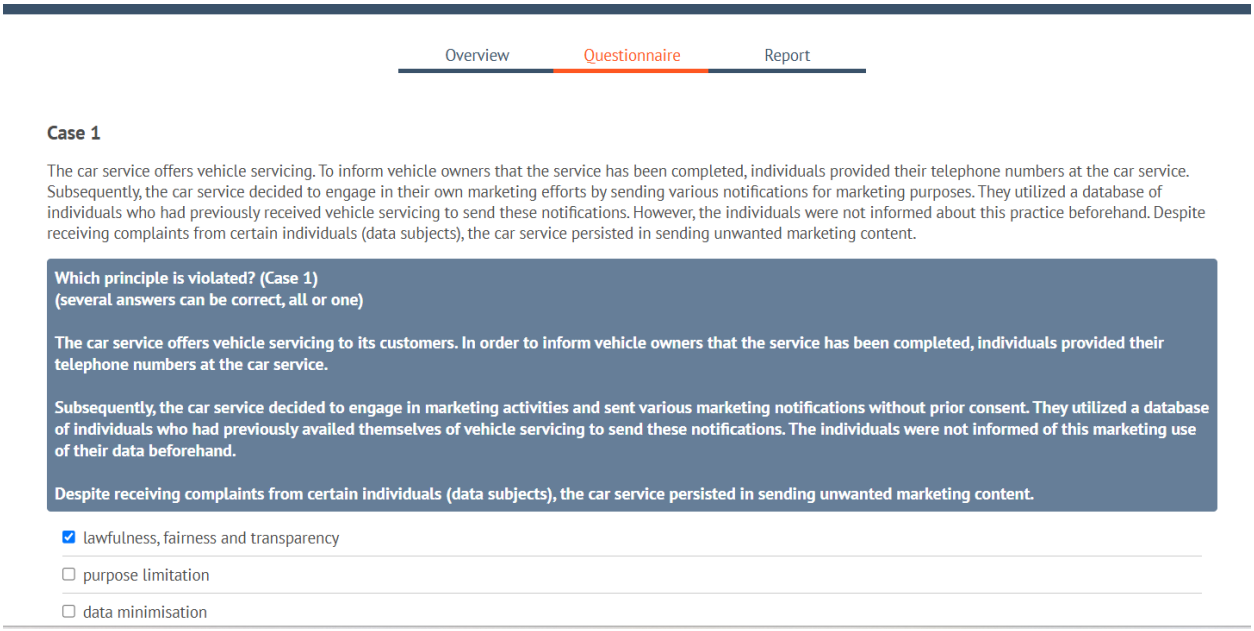


After watching the short educational video, there are 13 lessons that need to be studied in detail to master the material, after which we advise you to approach the knowledge test (Quiz).



If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.



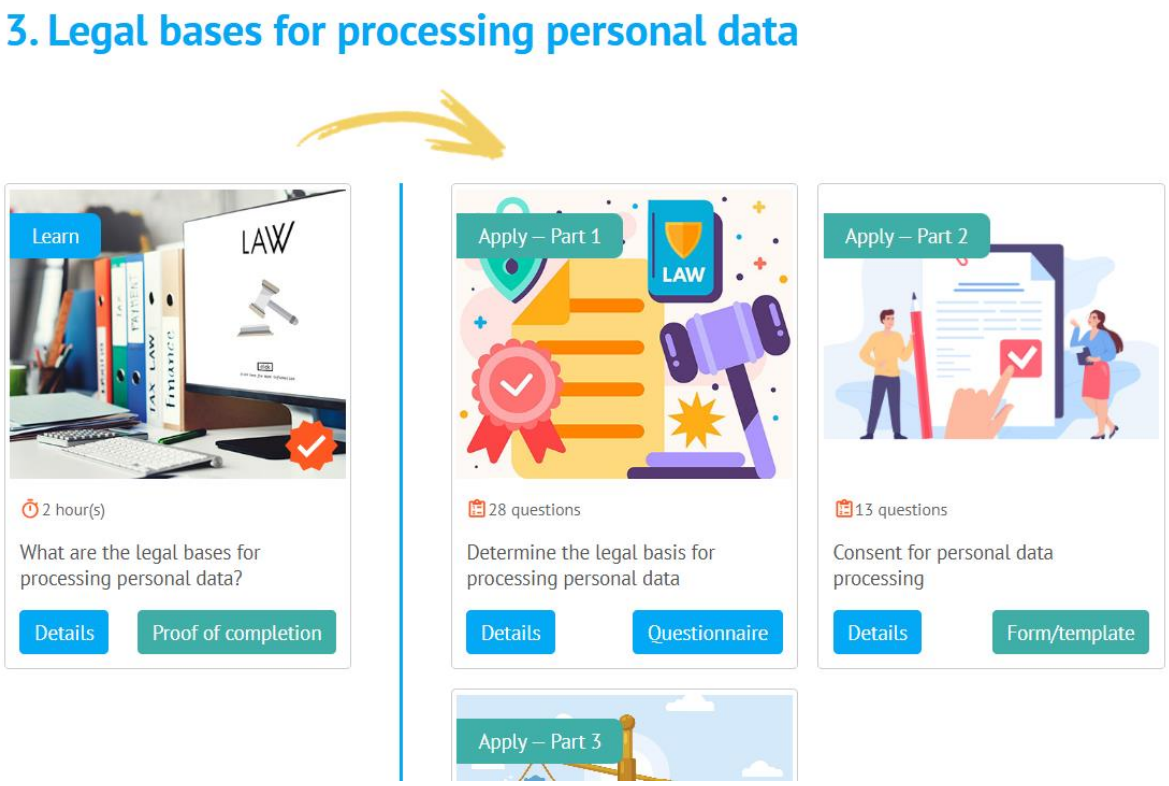


In the practical module on the principles of personal data processing, examples of personal data processing during which one or more principles of personal data processing have been violated are described. The objective of this practical module is to make it easier for SMEs to understand the principles set out in Article 5 of the General Data Protection Regulation through concrete practical examples.

After reading the description of the situation in which there was a violation of the principle(s) of personal data processing, it is necessary to identify which principle has been violated (one or more of them).

Your responses to the questionnaire can be saved and modified at any time. There is no limit to how many times you can complete or revise the questionnaire.

Once you have completed the questionnaire, you can download the report in .pdf format with answers and explanations.



The aim of the **"Legal Bases for processing personal data"** theoretical module is to familiarize users with the legal bases for the processing of personal data through practical examples in order to facilitate their understanding and application of different legal bases for the processing of personal data.

In this module, users have the opportunity to understand how to determine appropriate lawful basis through practical examples from various industries; identify different legal bases for the processing of personal data; describe the most common errors in determining the legal basis for the processing of personal data.

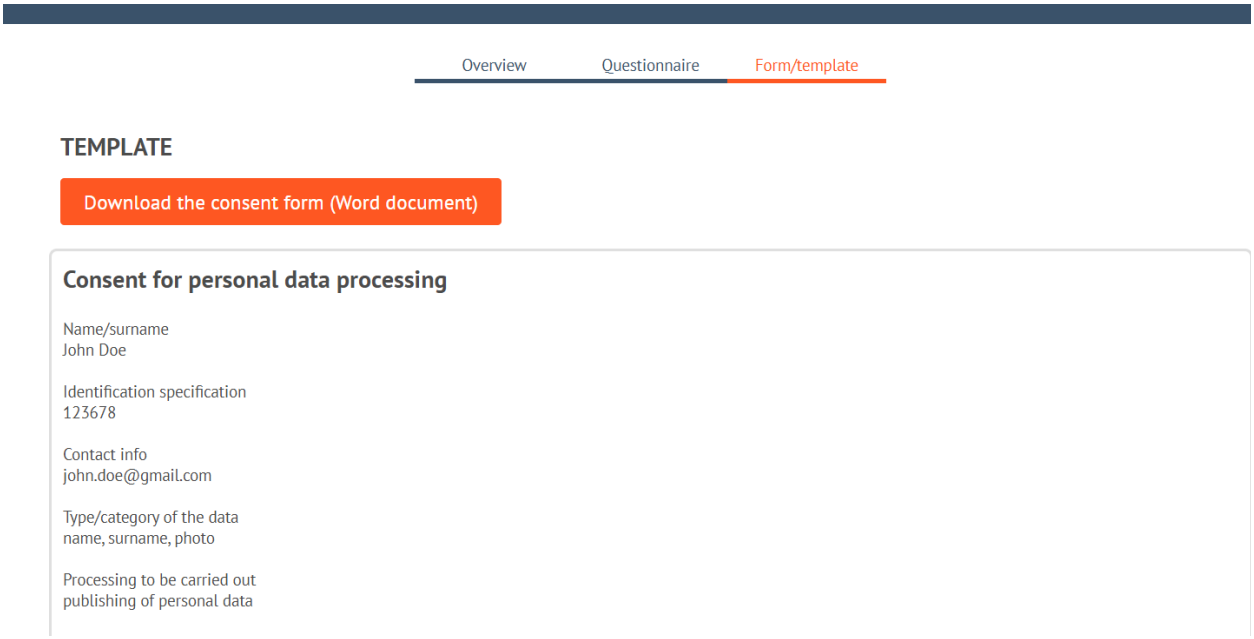
After watching the short educational video, there are 8 lessons that need to be studied in detail to master the material, and after that we advise you to approach the knowledge test (Quiz).

If you have more than 80%accurate answers, Olivia will generate a certificate of successful completion of the module.

The practical part of the "Legal Bases for processing personal data" course consists of 3 modules:

- An online form in which you can answer to questions related to processing activities in your organization. Once you have answered the questions, Olivia will generate a report that will help you identify the appropriate legal basis for the processing of personal data.

- Template for creating consent. If consent is the appropriate legal basis for the personal data processing activity you carry out, in this practical module you have the opportunity to fill out a form after which Olivia will generate a consent template in the form of a Word document. By using this template, you will ensure that the text of the consent complies with the requirements of the GDPR.



- Template for legitimate interest test (LIA). If you rely on a legitimate interest as a lawful basis, you are obliged to carry out a balance test to prove your legitimate interest. In this practical module, you have the opportunity to answer questions that will lead you to the conclusion whether you can rely on a legitimate interest as a legal basis for processing of personal data. Once you have answered the questions in the form, Olivia will generate a Word document that you will store to be able to prove your legitimate interest in the future.

GDPR topics › 3. Legal bases for processing personal data › Apply

Legitimate interest assessment

Overview | Questionnaire

STEP 1: Purpose test

An assessment of whether there is a legitimate interest in the processing of personal data.

*** Please describe in detail the reasons for which you want to process personal data:**

The Company (drugstore) conducts video surveillance at the Company's business address in accordance with Article 26 of the of the Croatian Act on the Implementation of the General Data Protection Regulation. Video surveillance is carried out for the purpose of protecting persons and property, based on a legitimate interest, the existence of which will be determined by this analysis.

The drugstore has so far reported several thefts and several physical attacks on the employees of the drugstore.

The purpose (reason for processing) is to reduce the risk of unauthorized entry into the business circle and to increase the protection and safety of employees and persons found on the Company's premises, especially entry/exit controls, and to reduce the exposure of employees to the risk of robbery, burglary, violence, theft. The purpose of the processing is also that a particular recording, in the event of a security incident, may be used as legal evidence in judicial or other proceedings and in the case of proof of damage for the purpose of securing persons and property.

*** What benefits do you expect from processing?**

should serve to prevent unlawful acts and video surveillance footage could serve as evidence in the proceedings in the event of such unlawful acts being committed.

We expect an increased level of safety of persons in the facility and the property of the company, which is the advantage of processing.

There is a benefit for all who work in the facility and visit the facility.

Processing is important for third parties because processing can identify the perpetrators of a wrongful act, e.g. lawyers need a recording as evidence in court proceedings; Insurance companies need a recording to prove the harmful event and the circumstances of the damage, the police to collect evidence in court proceedings.
Processing is necessary in order to increase the level of security of persons present on the facility, their property and the property of the Company. Video surveillance should serve to prevent unlawful acts and video surveillance footage could serve as evidence in the proceedings in the event of such unlawful acts being committed.

We expect an increased level of safety of persons in the facility and the property of the company, which is the advantage of processing.

There is a benefit for all who work in the facility and visit the facility.

Processing is important for third parties because processing can identify the perpetrators of a wrongful act, e.g. lawyers need a recording as evidence in court proceedings; Insurance companies

*** Do you comply with other relevant laws?**

YES, Labour act, GDPR and Act on the Implementation of the GDPR

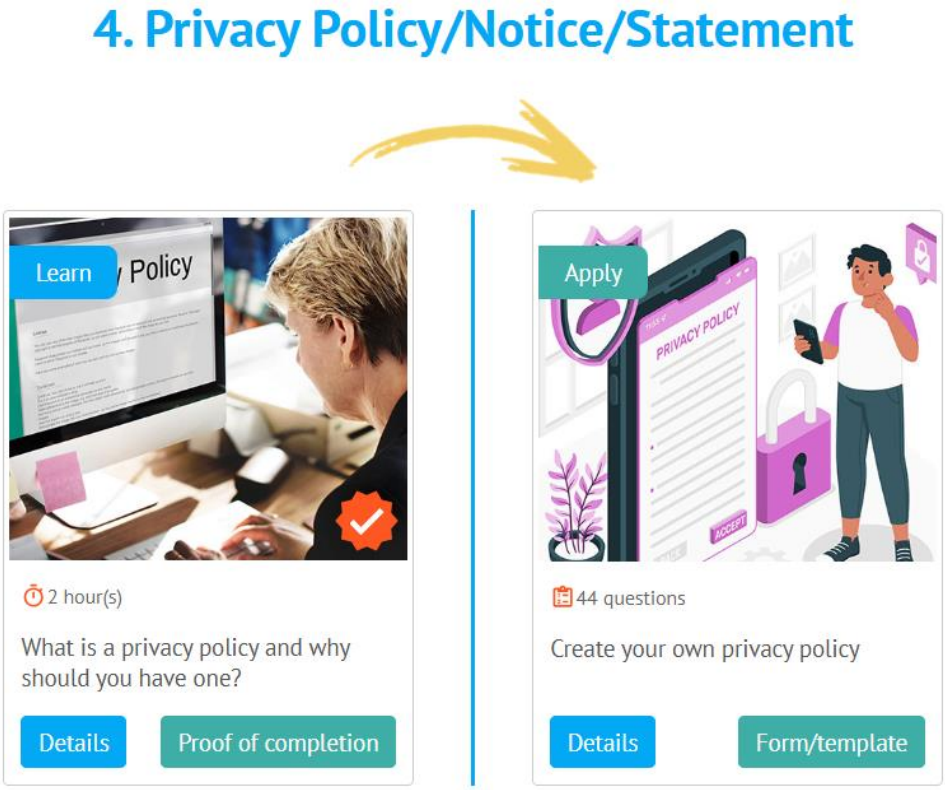
STEP 2: Necessity test

Assessment of whether processing is necessary for the purpose you have determined.

*** Will this process really help you achieve your purpose?**

YES. Processing is proportionate to the purpose and the purpose cannot be achieved in any other less intrusive way.

An alternative method exists but requires a disproportionate effort and investment. Recruiting several guards and establishing an internal protection service are possible alternatives, but they do not lead to easier and more efficient achievement of the goal. This possibility requires higher financial expenses, and in reality such a measure would be significantly disproportionate to the needs of the Company.



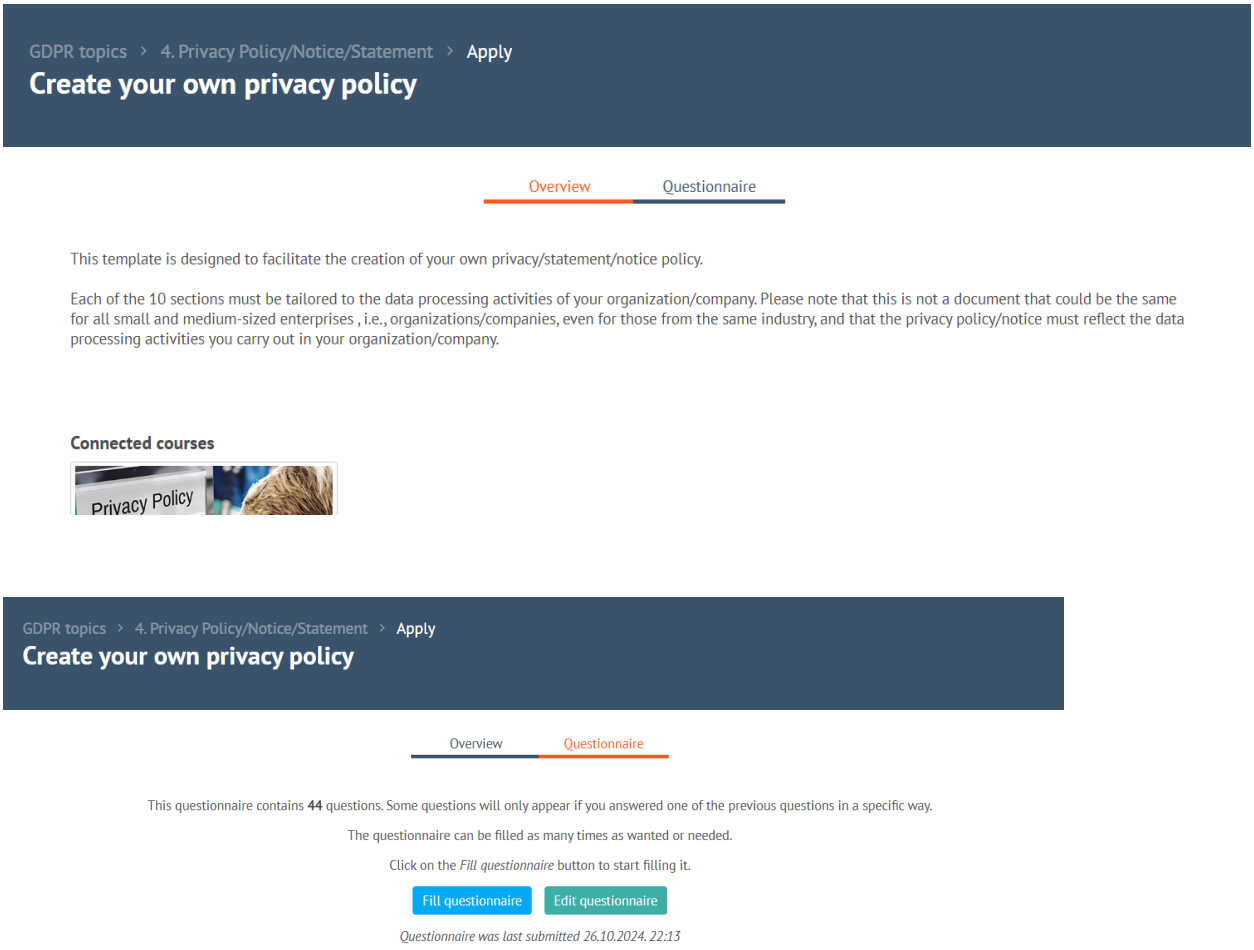
In the theoretical module of the course "Privacy Policy", users have the opportunity to learn why it is important to have an adequate privacy policy / statement on the processing of personal data or why it is important to inform data subjects about the processing of their personal data and how to create a privacy policy that will be in accordance with the General Data Protection Regulation (Articles 13 and 14 of the GDPR). General Data Protection Regulation).

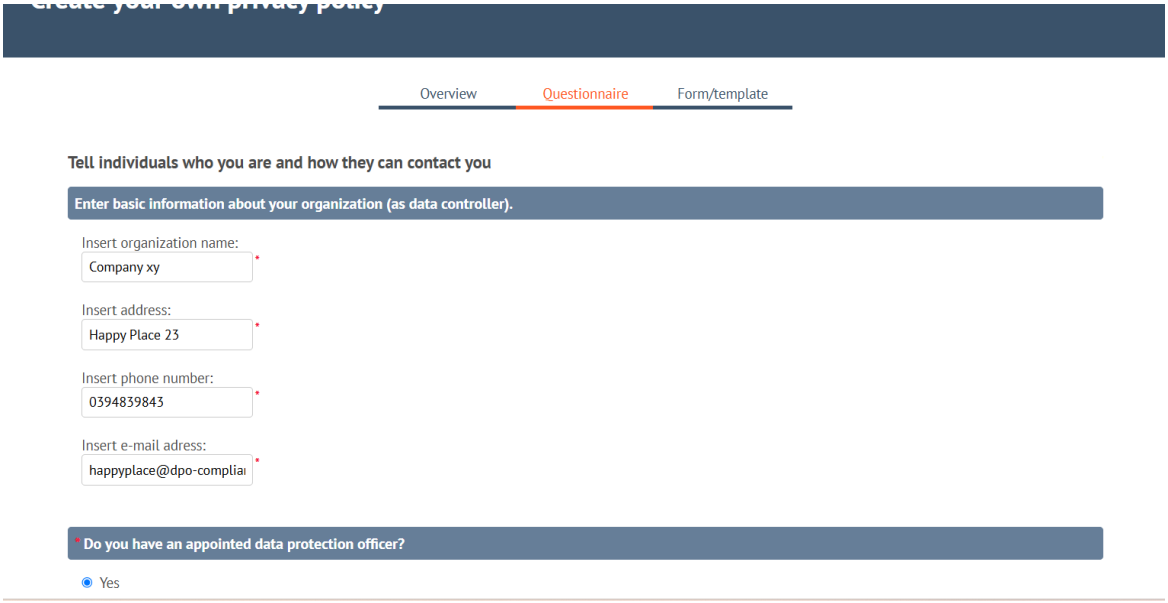
After watching the short educational video, there are **5 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

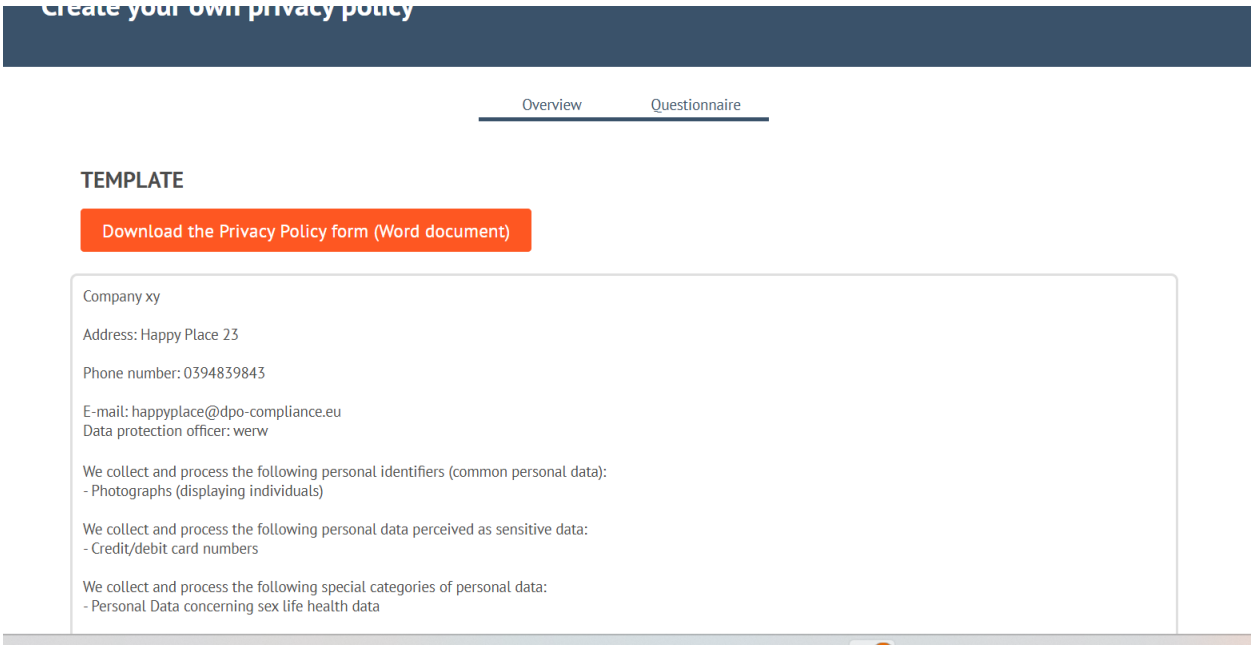
If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

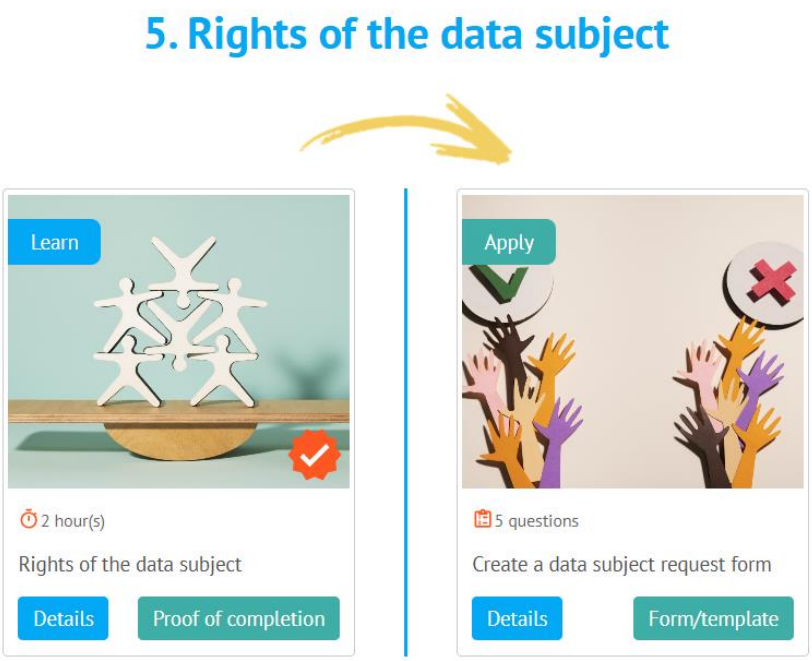
The practical part consists of an online form in which you need to enter accurate information regarding the processing activities you carry out, about which it is necessary to inform data subjects. Once you complete the form, Olivia will generate a privacy policy in the Word document. By using this template, which must be filled in correctly and contain accurate information related to processing activities in your organization, you ensure that data subjects will be provided with all the necessary information regarding the processing of their personal data. By clicking on the **"DOWNLOAD PRIVACY POLICY FORM"** button, you can download your privacy policy, save it to your computer, publish it on your website, send it to data subjects by e-mail or otherwise make it available to data subjects (your clients/service users). If you

want to change the answers you have entered in the online form, it is possible by clicking on the "**EDIT QUESTIONNAIRE" button.**




Overview
Questionnaire
Form/template
Tell individuals who you are and how they can contact you
Enter basic information about your organization (as data controller).
Insert organization name:
Company xy
Insert address:
Happy Place 23
Insert phone number:
0394839843
Insert e-mail adress:
happyplace@dpo-compliai
Do you have an appointed data protection officer?
Yes


Overview
Questionnaire
TEMPLATE
Download the Privacy Policy form (Word document)
Company xy
Address: Happy Place 23
Phone number: 0394839843
E-mail: happyplace@dpo-compliance.eu
Data protection officer: werw
We collect and process the following personal identifiers (common personal data):
- Photographs (displaying individuals)
We collect and process the following personal data perceived as sensitive data:
- Credit/debit card numbers
We collect and process the following special categories of personal data:
- Personal Data concerning sex life health data



In the theoretical module of the **"Rights of the data subject"** course, users will be able to learn and understand:

- what are the rights of the data subject and how are they related to the principles of personal data processing
- how to enable data subjects to exercise their rights and why this is of the utmost importance.

The aim of this theoretical module is to help users understand and understand the importance of data subjects' rights and how to meet data subjects' requests regarding the processing of their personal data.

Participants of this theoretical module will learn how to identify data subjects' requests regarding their rights to personal data protection and how to enable data subjects to exercise their rights.

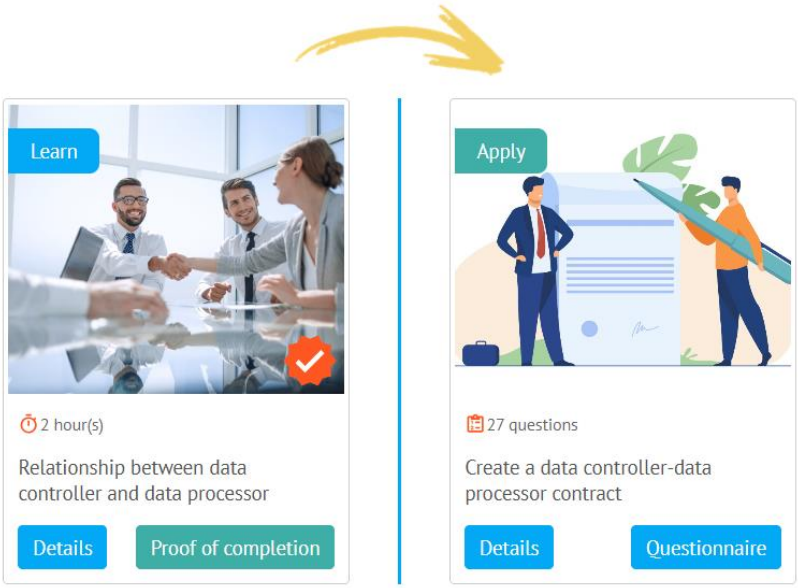
After watching the short educational video, there are **9 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

The practical part of the **"Rights of the data subject"** course consists of a form designed to make it easier for small and medium-sized enterprises (controllers) to enable their data subjects (clients, customers) to exercise their rights related to the protection of personal data. The enterprise (controller) fills in the fields name of the enterprise (organization), determines which personal data is necessary for him to meet his request and enters the contact details that the data subject can contact for the purpose of exercising his rights. The aim is to create a complete form for the exercise of the rights of data subjects, which will then

be publicly published by entrepreneurs (controllers) on their websites or will be available to data subjects at the business premises of the controller, which will make it easier for entrepreneurs to obtain a correct and complete request, and for data subjects to exercise their rights.

6. The relationship between data controller and data processor



In the theoretical part of this course, users can learn and understand:

- who is the controller, who is the processor, who are the joint controllers and what are their mutual obligations;
- who are the recipients of the personal data, third parties and sub-processors;
- how to regulate the relationship between controller and processor

The aim of the theoretical module is to help entrepreneurs/users to define their role in the process of processing personal data: whether they are controllers, processors, joint controllers or third parties and recipients. If they are controllers and have processors, such relationships must be governed by a contract or other appropriate legal act.

After watching the short educational video, there are **11 lessons** that need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

The practical module consists of an online form that assists controllers in drafting the Agreement on the processing of personal data between the controller and the processor pursuant to Article 28(3) of the GDPR. General Data Protection Regulation.

After completing the questionnaire, a template contract for the processing of personal data will be generated in the form of a Word document. Please note that users will need to adjust the text of the contract to be used in their business, depending on the needs and specifics of individual processing, and the template in no way represents a guarantee that the processing of personal data is in accordance with the General Data Protection Regulation.

In this theoretical module of the course **"Records of processing activities"**, users can learn what personal data processing activities are and how to keep them, what are the advantages of up-to-date and correct record keeping of processing activities, what it must contain and in what circumstances are processing managers obliged to keep records of processing activities.

All data controllers should keep records of processing activities, as it is an overview of all personal data processing activities in an organisation and serves as an excellent tool for demonstrating compliance with the General Data Protection Regulation.

In short, users will have the opportunity to learn in this module:

- identify whether there is a legal obligation to conduct processing activities
- understand that a record of processing activities is one of the tools to demonstrate compliance with the GDPR and that it is desirable to keep a record even when this is not a legal obligation;
- describe what the records of processing activities must contain.

After watching the short educational video, **there are 10 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

The practical module consists of two parts:

- **an online form to assist data controllers in creating a** record of processing activities in accordance with Article 30, paragraph (1) of the GDPR

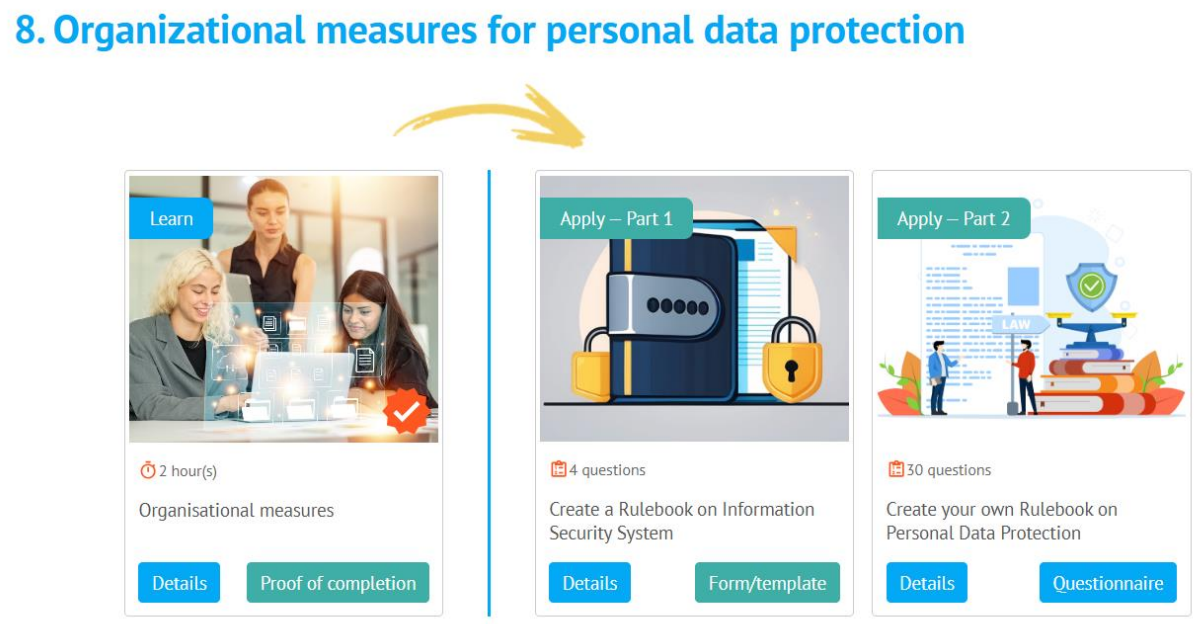
- **an online form to assist data processors** in creating a record of categories of processing activities in accordance with Article 30, paragraph (2) of the GDPR

Once the questionnaire is completed, a template for the record of processing activities/records of categories of processing activities in Excel format will be generated.

You can download this document by clicking on the "Download form" button.

As the processing activities of your organisation will change over time, the records of processing activities/records of categories of processing activities will also need to be updated accordingly.

You can download, save to your computer and modify the records in Excel format, and it is possible to make changes in Olivia, by clicking on the EDIT QUESTIONNAIRE button.



In the theoretical module of the course "Organisational measures for the protection of personal data", users can learn that the choice of appropriate organizational measures depends on the risk of personal data processing (small, medium, high, very high). In addition, Olivia explains which internal acts need to be developed to demonstrate accountability (compliance with the General Data Protection Regulation).

The aim of this module is to teach users (controllers) how to apply appropriate organizational measures to protect personal data in their organizations.

Learning outcomes:

- identify the risks associated with the processing of personal data;
- understand what organizational measures to protect personal data need to be taken in order for personal data to be adequately protected
- describe the internal acts that need to be developed to demonstrate compliance with the GDPR
- Recognize the importance of education on personal data protection of all employees in the organization.

After watching the short educational video, there are **4 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

The practical part of the course "Organisational measures for the protection of personal data" consists of two online forms:

- online form for drafting the Rulebook on Information Security

This template is designed to make it easier for you to create an Information Security System Policy. The answers to all the questions in this must be in accordance with the specific data processing activities in your organisation/company. Please note that this is not a document that is the same for all SMEs, not even for organisations/companies from the same industry.

The information security system policy must be adapted to the data processing activities you carry out in your organisation/company, i.e. it must reflect the actual measures and procedures taken by the controller/processor to prevent loss or unauthorised disclosure and to remedy the consequences in the event of loss or unauthorised disclosure of the personal data it processes.

- online form for drafting the Personal Data Protection Policy

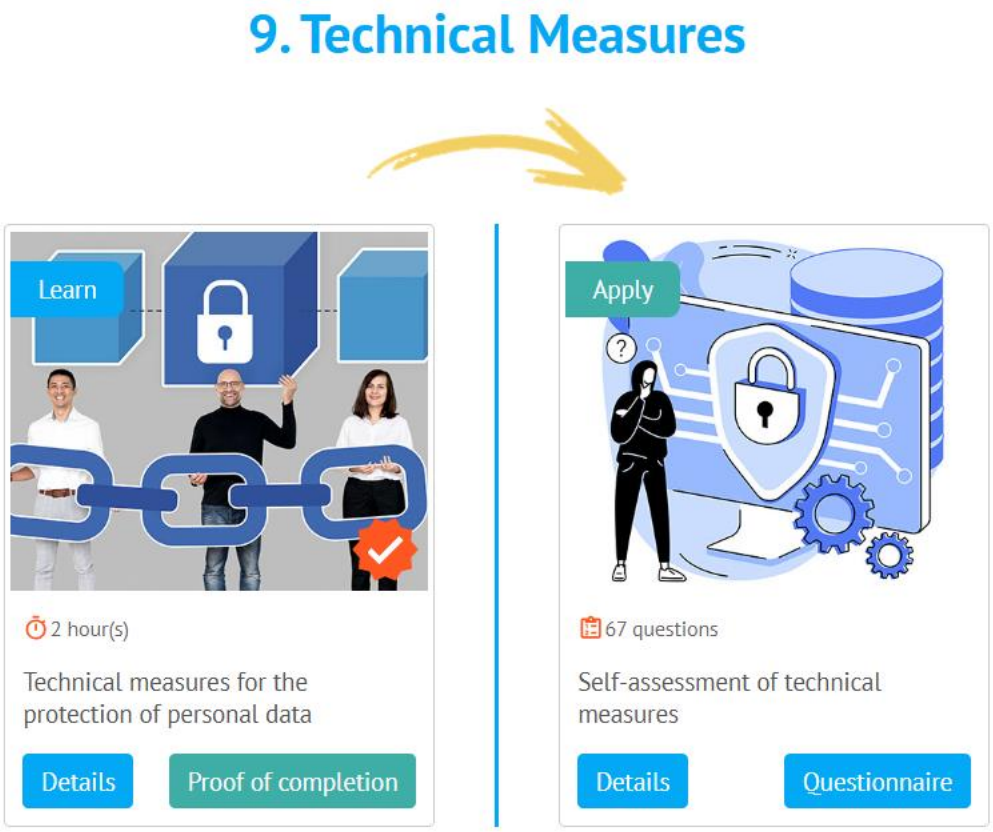
This template is designed to make it easier for you to create a Personal Data Protection Policy.

The answers to all questions in this online form (template)must be tailored to the data processing activities in your organisation/company. Please note that this is not a document that is the same for all SMEs, i.e. organisations/companies, even those from the same industry.

The Personal Data Protection Policy must be tailored to the data processing activities you carry out in your organisation/company.

This policy is intended for internal use only by employees of the data controller. It is not designed for public distribution or to inform data subjects about the processing of their personal data. Instead, this policy serves

as a comprehensive guide for all employees who handle personal data, ensuring they understand and adhere to the principles of lawful, fair, transparent, and secure data processing. By familiarizing themselves with the contents of this policy, employees will be equipped to manage personal data in compliance with applicable data protection regulations and best practices.



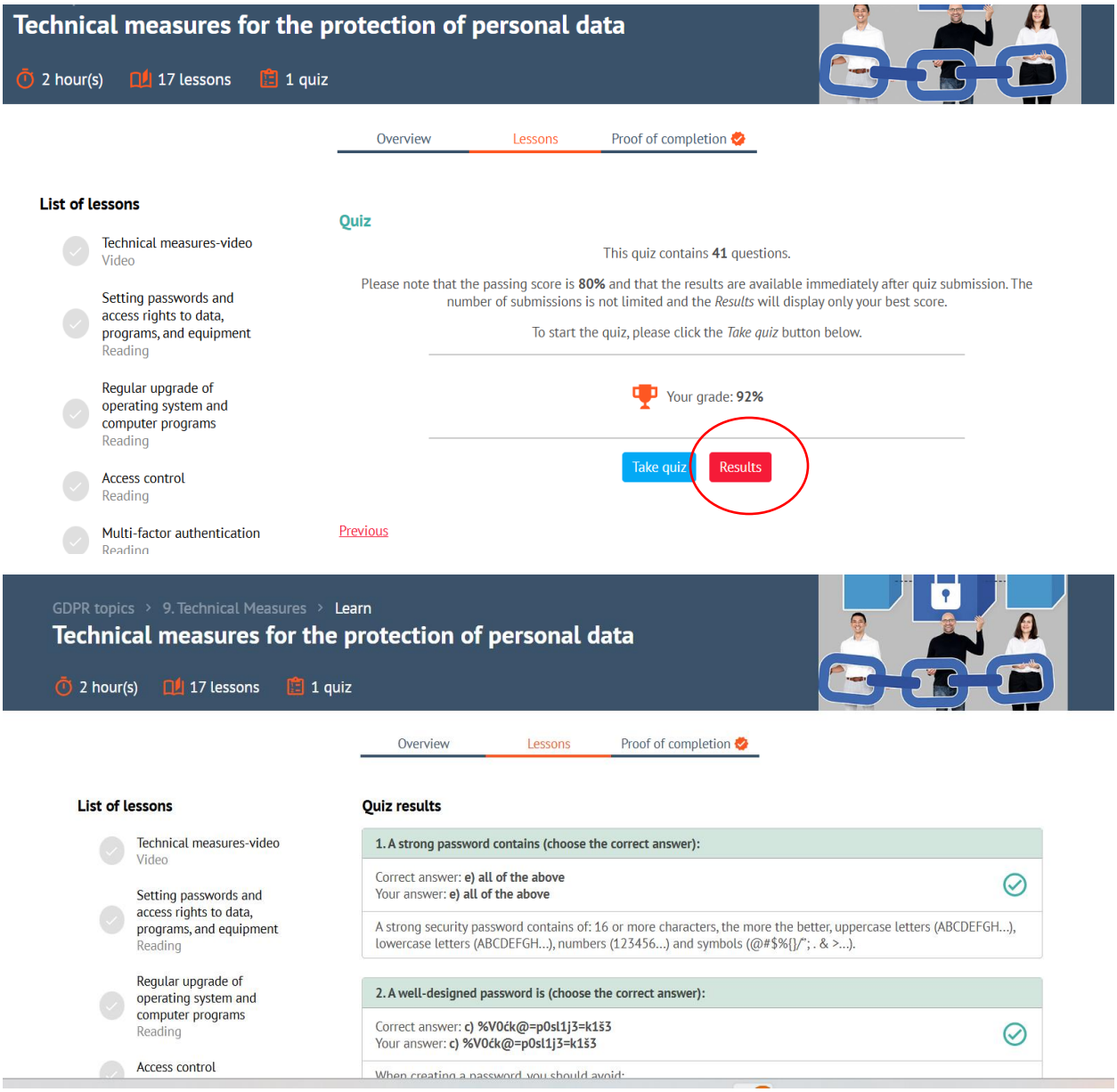
In the theoretical module of the course **"Technical measures for the protection of personal Data,"** you can learn what technical measures exist for the protection of personal data, how to assess risks, and how to take appropriate measures. The aim of this theoretical module is to familiarize users with the importance of applying appropriate technical measures, how to assess which measures are adequate, and understand the interdependence of technical and organizational measures.

Learning outcomes

- understand what technical measures of personal data protection are
- identify the appropriate technical measures to be applied by the controller in its business operations;

After watching the short educational video, there are **16 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.



The practical part of the course "Technical measures for data protection" consists of a questionnaire for self-assessment of the level of security of processing in the organization. **This self-assessment questionnaire for the level of personal data security consists of 67 data protection measures, and in relation to each offered measure you have the opportunity to respond with: YES; NO; NOT APPLICABLE.**

Article 32 of the GDPR deals with the security of personal data processing and requires controllers and processors to implement appropriate technical and organisational measures to ensure an appropriate level of security.

The technical and organisational measures referred to in Article 32 of the GDPR are intertwined in several ways, i.e. technical measures often depend on organisational measures and vice versa. For example, the implementation of encryption software (technical measure) requires appropriate key management policies and procedures (organisational measure).

IMPORTANT NOTE: This self-assessment questionnaire is for the sole purpose of indicating to data controllers and data processors some of the basic technical and organisational measures they should take to protect the personal data of their users/clients/employees.

If a specific measure from the self-assessment questionnaire is not applicable to your business (for example, your employees do not use smartphones and tablets for business purposes, do not use the services of the data processor, e.g. to store personal data in the cloud, etc., your answer should be NOT APPLICABLE (N/A).

If you have implemented a certain measure for the protection of personal data, then your answer should be YES. If not, and the measure is applicable to your processing activities, the answer should be NO.

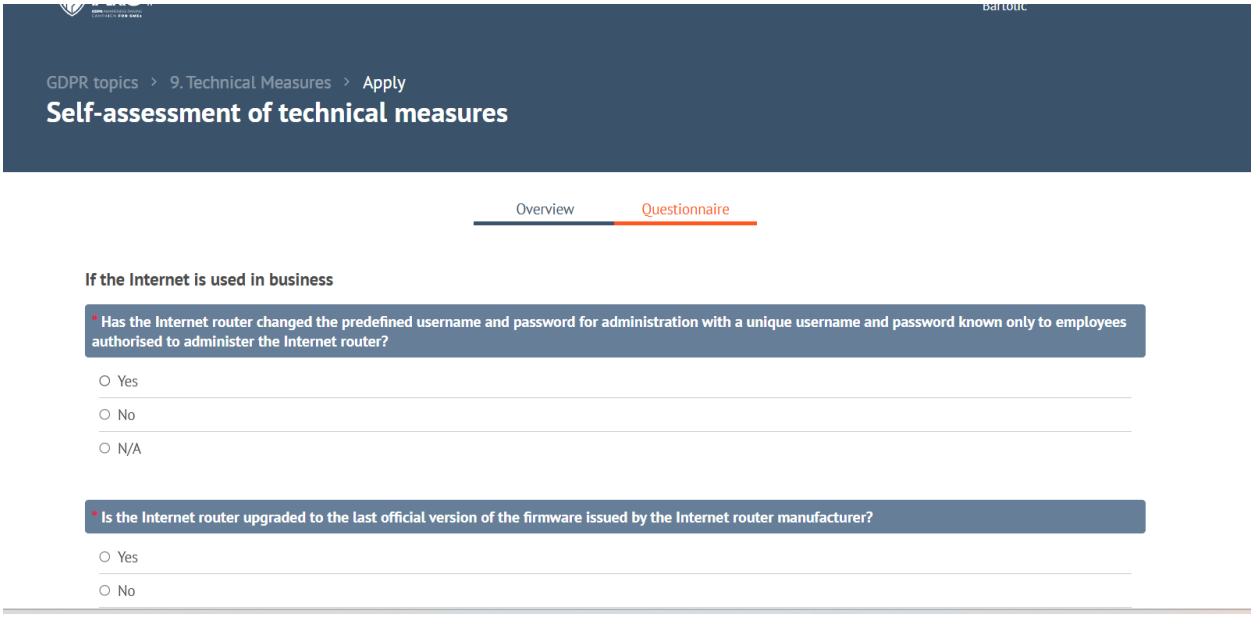
The goal you need to achieve is YES answers to all applicable measures to achieve a basic level of security for the processing of personal data in your organisation.

It is crucial to emphasize that this questionnaire covers only the fundamental measures for ensuring an adequate level of data protection. It does not encompass all possible measures a data controller might implement. The specific measures required will vary based on the risk level associated with the data processing activities undertaken.

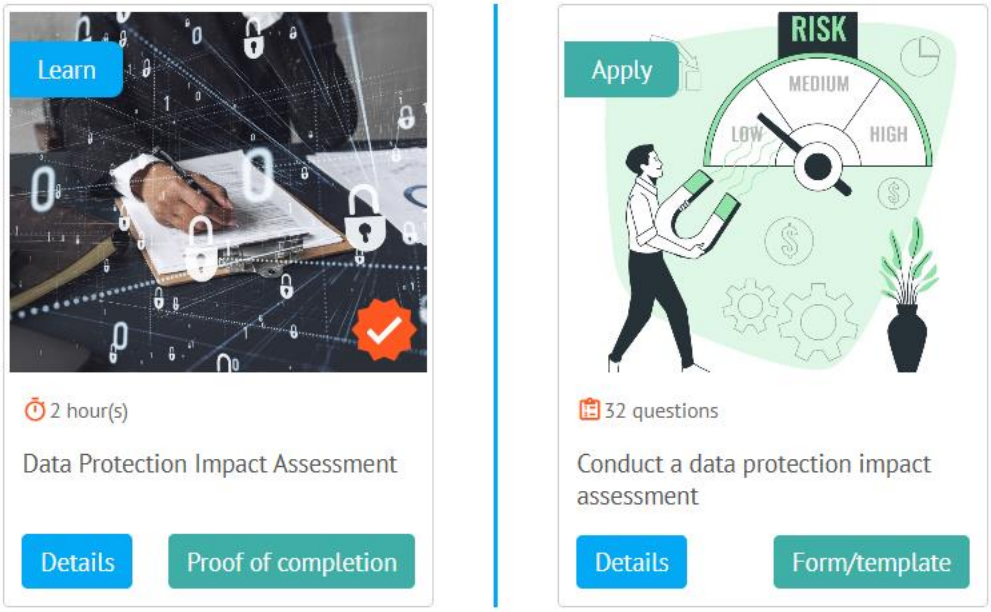
Furthermore, it's essential to recognize that 'appropriate measures' are a context-dependent term. What constitutes appropriate measures will differ significantly among data controllers based on factors such as the nature of their business, the volume and sensitivity of data processed, and the potential risks involved. For instance, the appropriate measures for a financial institution like a bank would be markedly different from those required for a small retail business such as a flower shop.

Data controllers should use this questionnaire as a starting point and supplement it with additional measures tailored to their specific data processing activities and associated risks. Regular risk assessments and staying informed about evolving data protection best practices are recommended to maintain an effective data protection framework.

After completing the self-assessment questionnaire, by clicking on the **"DOWNLOAD REPORT" button, you can download the report in .pdf format** and find additional explanations for each of the above measures.



10. Data protection impact assessment (DPIA)



In the theoretical module of the course "Data Protection Impact Assessment", you have the opportunity to learn in which cases you are obliged to carry out a data protection impact assessment, which criteria are taken into account when assessing whether the processing of personal data will result in a high risk to the rights and freedoms of natural persons and what the impact assessment must contain and who is responsible for carrying out the data protection impact assessment.

The aim of this theoretical module is to teach entrepreneurs that processing activities are subject to the requirement for a data protection impact assessment, why it is important to carry out the same in cases of high-risk processing, what needs to be taken to reduce the risk and what are the negative consequences that can occur if the impact assessment is not carried out or is not carried out properly.

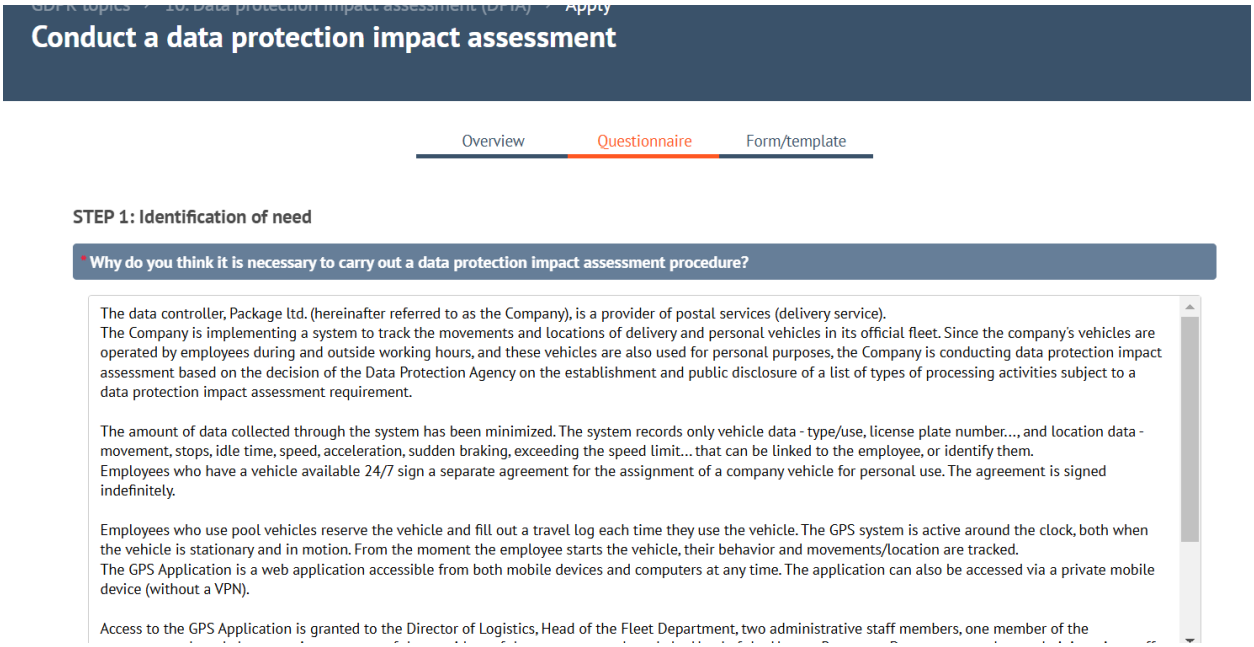
Learning outcomes

- identify the personal data processing activities that require a data protection impact assessment;
- understand the criteria to be taken into account when assessing which processing operations are likely to result in a risk to the rights and freedoms of natural persons;
- describe what and why the data protection impact assessment must contain.

After watching the short educational video, there are **11 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

In the practical module of the "Data Protection Impact Assessment" course, you can find an online form with questions that will help you conduct a data protection impact assessment. Once you have completed the information form regarding the description of the processing operations you intend to carry out, the assessment of the necessity and proportionality of the processing operations to their purposes, the identification of the risks and the appropriate measures to address the risks, Olivia will generate a template in a Word document that you can download by clicking on the **"Download Template" button.** You can store the template on your computer in word and .pdf format and change it if necessary, and changes can be made in the practical module itself.



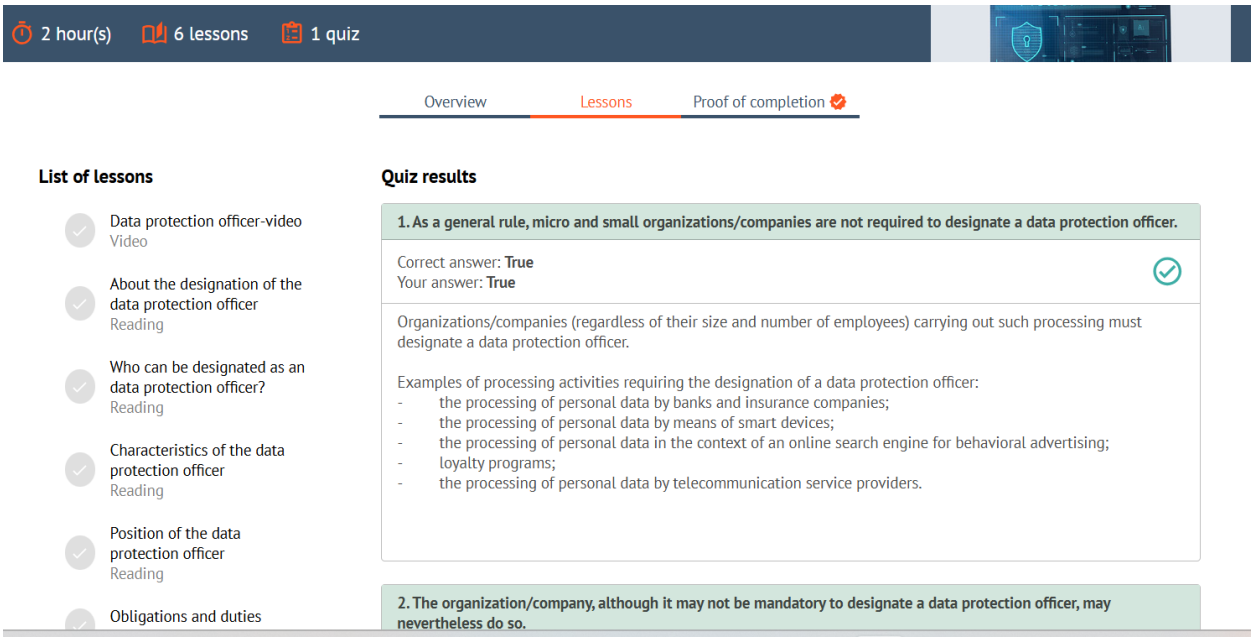
In the theoretical module of the course **"Data Protection Officer"**, you have the opportunity to learn under which circumstances you are obliged to appoint a Data Protection Officer (DPO), what the duties of a DPO are, and what qualifications and qualities a DPO must have in order to perform tasks in a quality manner. The aim of this theoretical module is to familiarize users with the role of the data protection officer in the organization/company, the situation in which DPO appointment is prescribed and his/her characteristics and duties, as well as the obligations of organizations/companies in relation to him/her.

Learning outcomes

- Understand the role of the DPO in the organisation/company
- Identify the characteristics and duties of the data protection officer;
- Describe the situations in which the appointment of data protection officers is mandatory
- How to avoid the Data Protection Officer being in conflict of interest

After watching the short educational video, **there are 5 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.



The practical part of the **"Data Protection Officer"** course consists of two online questionnaires.

- **The first self-assessment questionnaire consists** of questions that will help you decide whether you are obliged to appoint a data protection officer. Answer the questions **YES** or **NO**, depending on which of the above statements is applicable to your organisation.

authorities. This appointment helps to ensure transparency, accountability, and the protection of individuals' rights in relation to their personal data.

4. Our core business includes some forms of online tracking and profiling of a large number of individuals for the purposes of behavioral advertising.

Yes

Description:

You are obliged to designate a data protection officer because:
- your core business consists of processing operations which, by reason of their nature, scale and/or purposes, require **regular and systematic monitoring of data subjects on a large scale**, or
- it is possible that your core business also consists of **large-scale processing of special categories of data.**

"Regular and systematic monitoring" of organization/company certainly includes all forms of monitoring and profiling. The concept of tracking is not limited to the internet environment, which is one of the examples of monitoring the behaviour of respondents.

What is meant by the processing of personal data on a "largescale"?

Factors taken into account when assessing whether personal data are processed on a large scale: the number of individuals, the scope of the personal data processed, the duration of the personal data processing activities and their geographical scope.

5. One of the tools that my organisation/company uses in its business is a loyalty program.

Yes

Description:

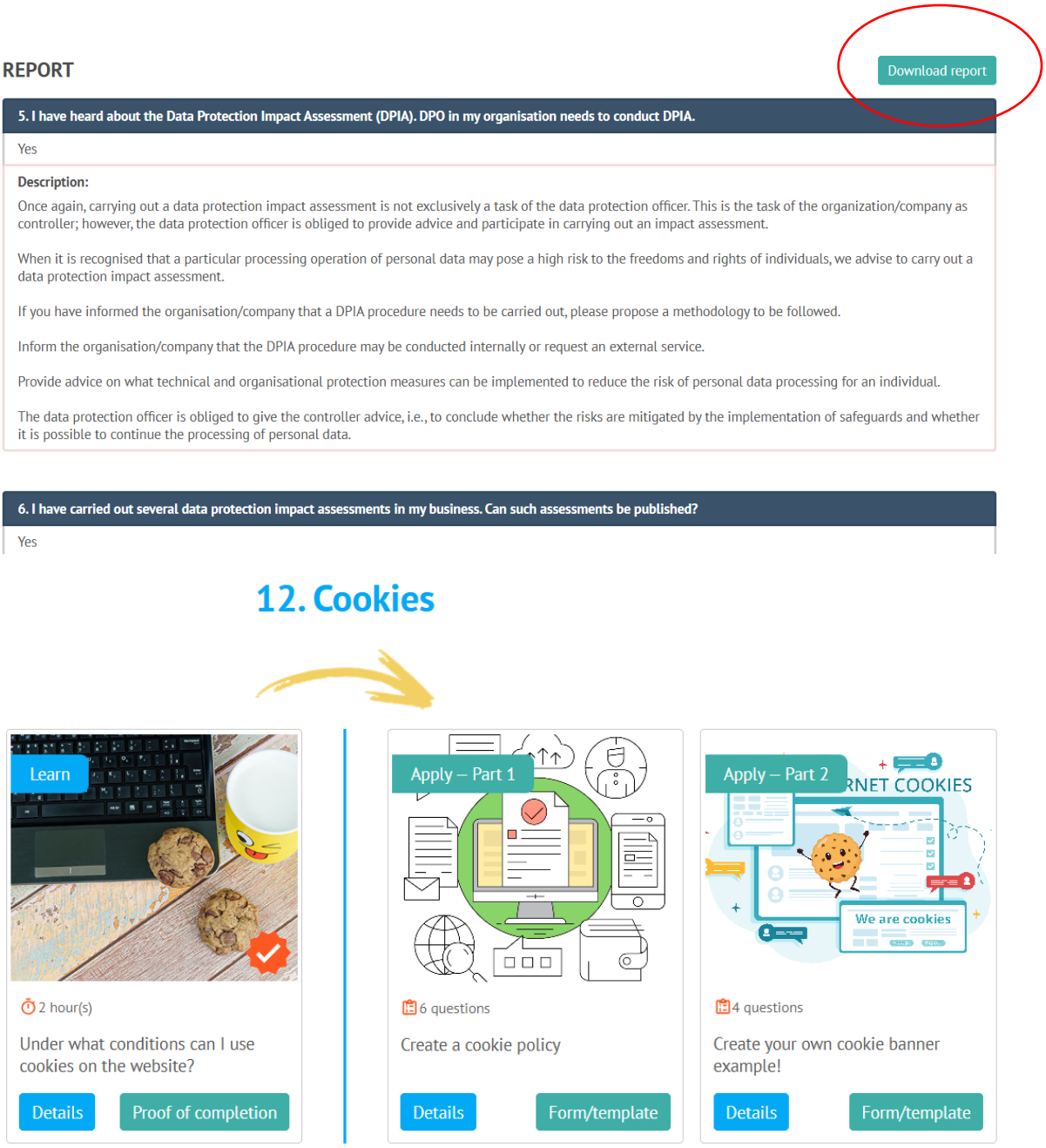
The use of loyalty programs is considered to be a "regular and systematic monitoring" of individuals.

IMPORTANT NOTICE! Please note that the questionnaire provides only a few examples of when an organization is obliged to appoint a DPO. If the activity in which your organization is engaged is not included in the questionnaire or none of the above examples apply to your organization, this does not mean that you are under no obligation to appoint an official.

The second self-assessment questionnaire consists of questions to help you better understand the conditions for appointment and the position and tasks of the DPO.

Answer the questions **YES** or **NO** according to the actual situation in your organisation.

Once you have answered all the questions, by clicking on the **"Download report"** button, you can download the answers you provided in the questionnaire to your computer, which will be accompanied by explanations.



In the theoretical module of the course "Processing of personal data through cookies", you have the opportunity to learn what cookies and tracking technologies are, what types of cookies exist and for what purpose they are used, about consent as a legal basis for the processing of personal data through cookies, what conditions should be met by such consent and how to inform data subjects about the processing of their personal data through cookies.

Learning outcomes

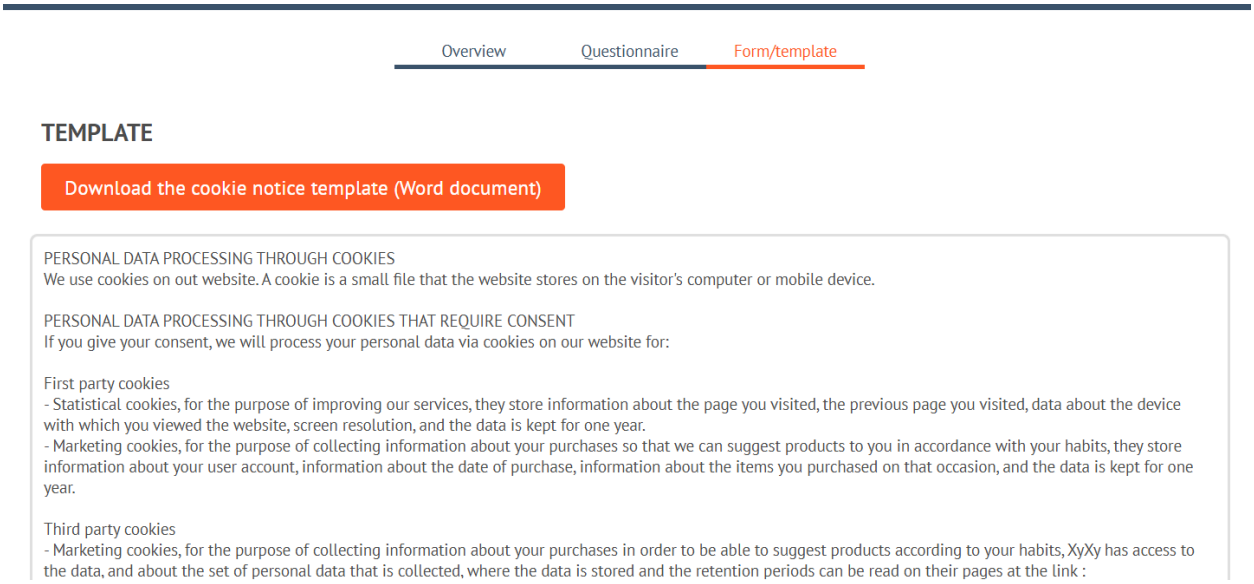
- understand what cookies and other tracking technologies are, what types exist and for what purpose they are used
- identify legal regulations governing the processing of personal data through cookies and other tracking technologies
- create a "cookie banner" in accordance with the requirements of the General Data Protection Regulation
- create a cookie policy (information about the processing of personal data through cookies intended for data subjects) in accordance with the General Data Protection Regulation
- how to check which cookies are used on the website.

After watching the short educational video, there are **5 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

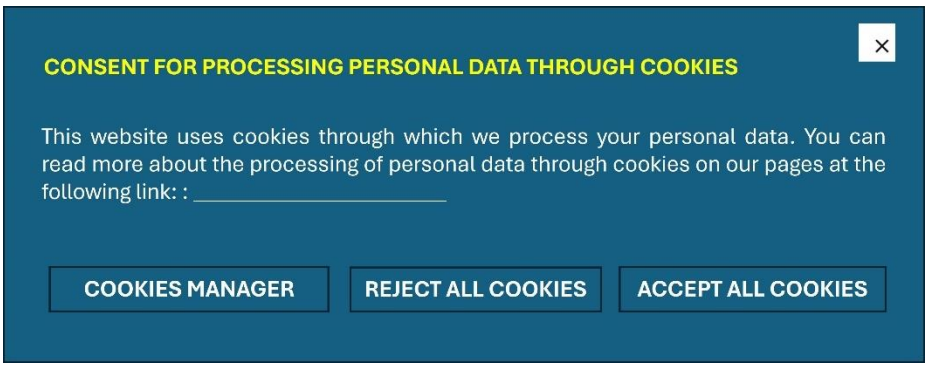
The practical part of the course "Processing of personal data through cookies" consists of two online forms:

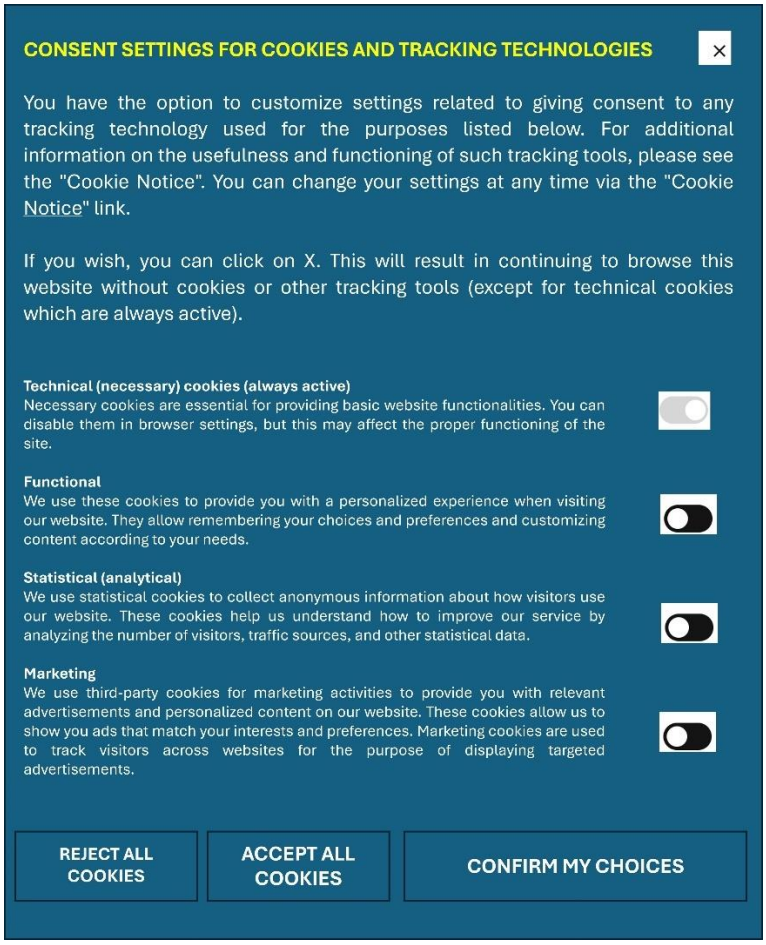
- create an online form for creating a cookie notice . After answering the 7 questions in the questionnaire, you have the option of downloading a notification called **"Cookie Notice" in the form of a Word document by clicking on the button "DOWNLOAD THE COOKIE NOTICE TEMPLATE".**



It is important to note that this information should describe the actual state of the website, i.e. the actual types and categories of cookies, which personal data are actually collected using these cookies, what is their actual purpose and storage periods, who has the right to access the data stored in cookies and whether data is transferred to third countries or international organisations.

- **online form (questionnaire) for creating a consent form for processing personal data through cookies (so-called cookie banner).** After answering the 4 questions in the questionnaire, in case you process personal data through cookies for which consent is required, you are obliged to ask the visitor's consent via the bar or pop-up *window about the consent to the processing of personal data through cookies (cookie banner/pop-up cookie consent).*



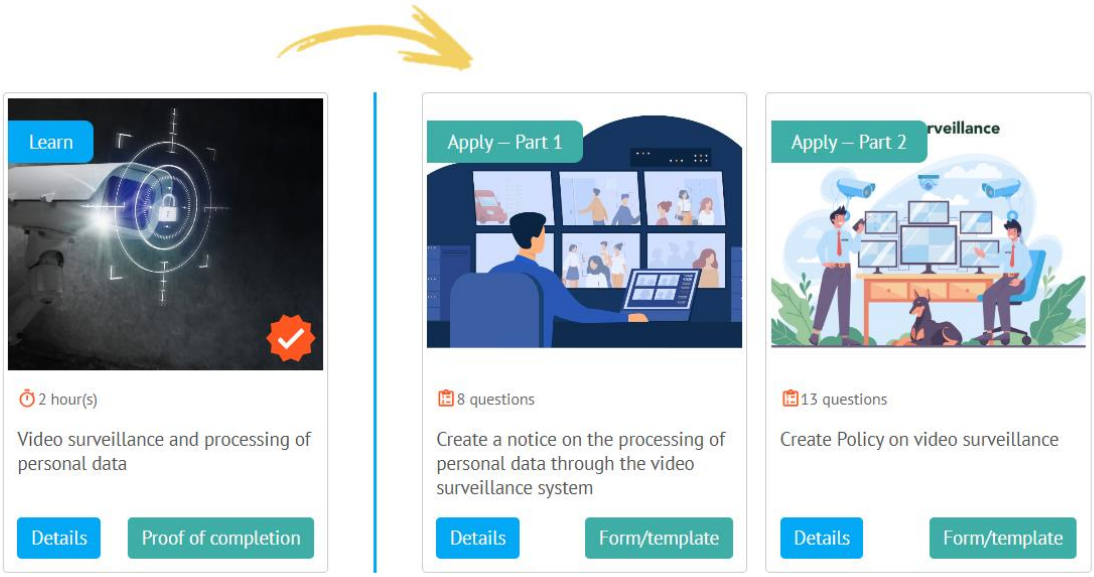


Olivia will generate an example of a cookie bar/pop-up window based on your answers in the questionnaire. This bar/pop-up window is not fully functional and serves only as an example of what your "cookie banner" should look like or contain.

In addition, the example that you can download by clicking on the ***Download Example*** button above contains a code for a non-functional bar/pop-up window that can be used as a basis for implementing a fully functional version.

Click on the ***Cookie Settings*** button to open additional options to customize your own cookie settings.

13. Video surveillance and processing of personal data



In this theoretical module, you have the opportunity to learn what are the **legal bases for the processing of personal data through a video surveillance system, under which conditions it is allowed to record employees in the workplace, which must include a notice of video surveillance, who has the right to access video surveillance recordings, how long recordings can be stored, under which conditions it is allowed to monitor workers through GDPS, under which conditions the processing of biometric personal data in the private sector is allowed.**

The aim of this theoretical module is to familiarize users with the legal grounds for the processing of personal data through a video surveillance system, to point out to them situations when such processing is not lawful and to teach them how to regulate the processing of personal data through a video surveillance system (which should include a notice of video surveillance intended for persons affected by the video surveillance system, define who has access to the recordings, record who accesses the recordings, ensure that the recordings have access only to authorised persons, do not keep the recordings for more than 6 months, etc.)

Learning outcomes

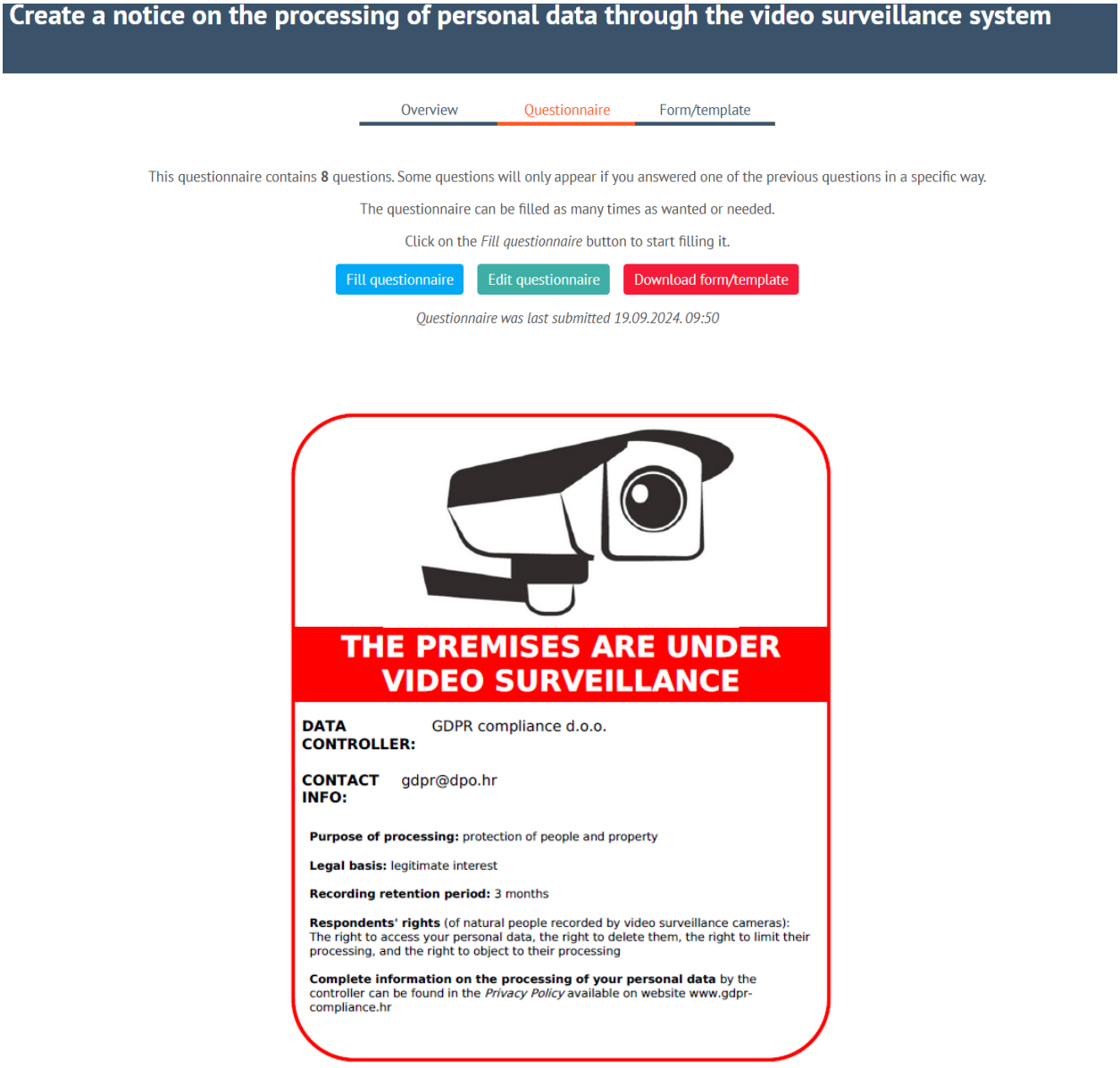
- understand under what conditions the processing of personal data by video surveillance is lawful
- identify the appropriate legal basis for the processing of personal data through the video surveillance system;
- describe what must be included in the Rules on video surveillance and notice of video surveillance intended for respondents.

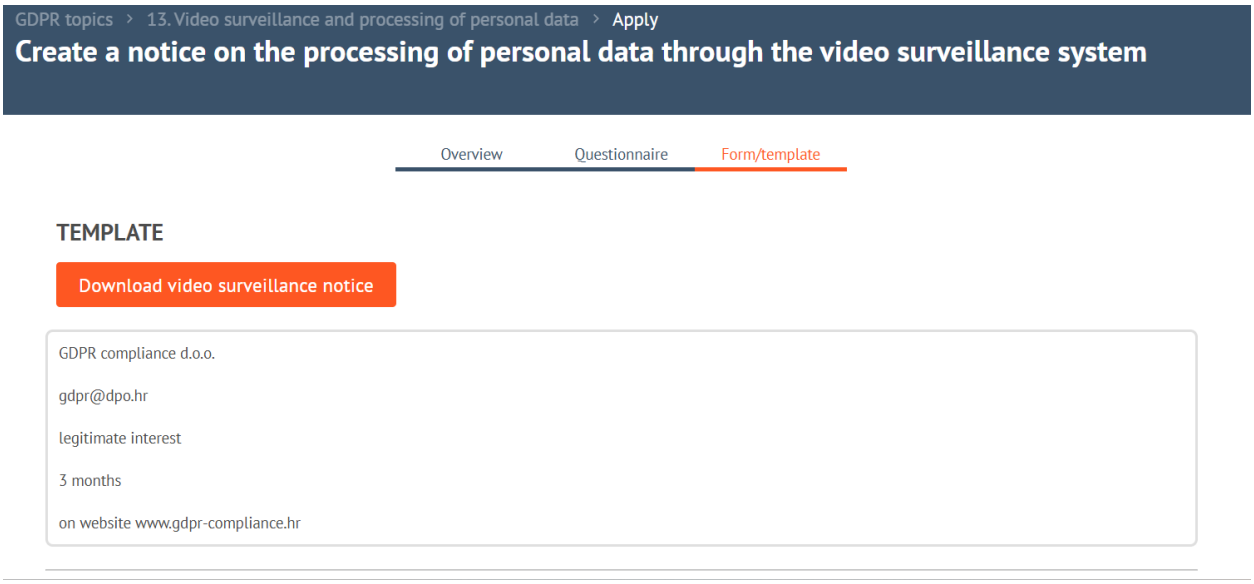
After watching the short educational video, there are **10 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

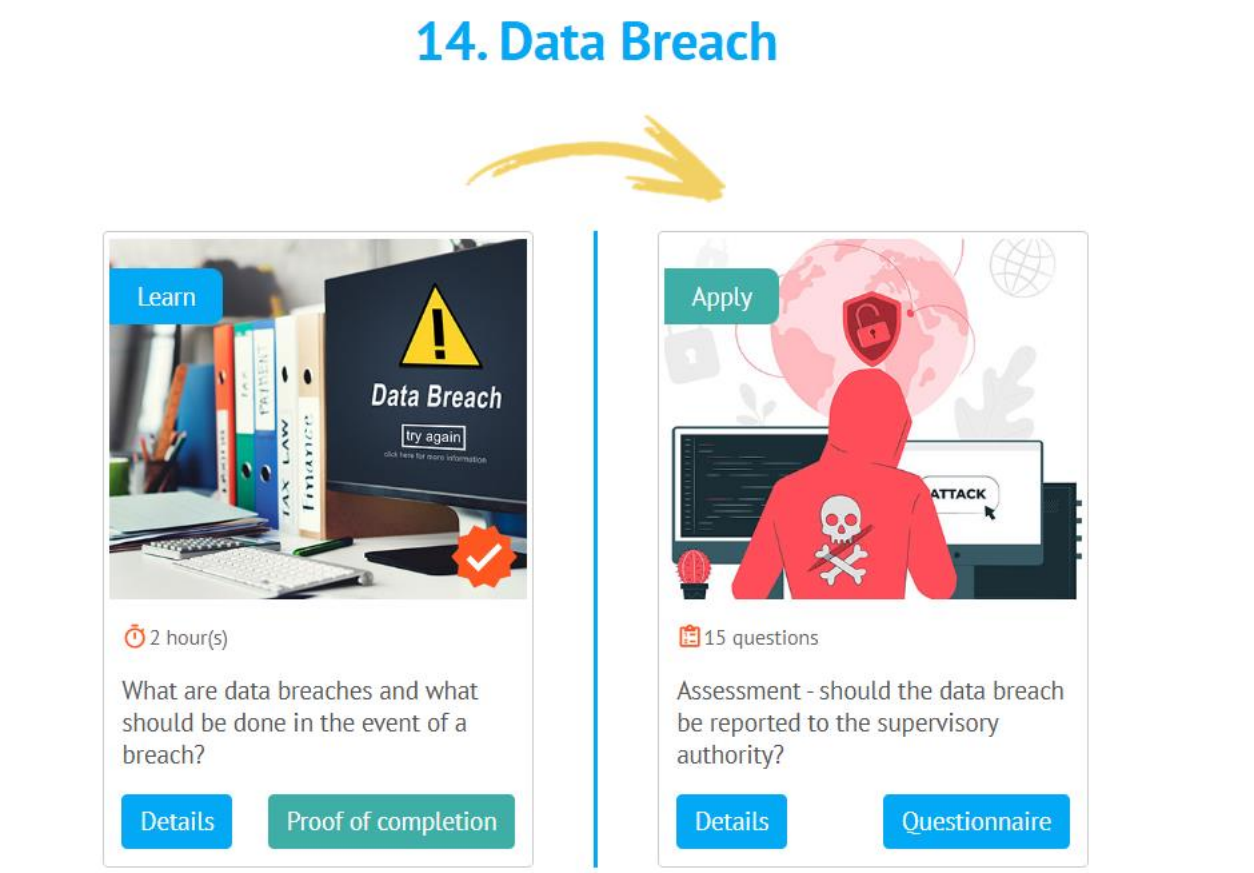
If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

Practical module of the course **"Processing of personal data by means of video surveillance; biometrics; worker tracking via GPS' consists of two online forms (questionnaire):**

- online form (questionnaire) used for creating video surveillance notices. After answering **11 questions from the questionnaire**, according to your answers, Olivia will generate a video surveillance notice in .pdf format. You can download the notification by clicking on the **"Download form/template"** button.







In this theoretical module, you can learn about your obligations as a controller or processor in the event of a personal data breach.

In the event of a personal data breach where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controllers shall without undue delay and, where feasible, not later

than 72 hours after having become aware of it, notify the supervisory authority (Personal Data Protection Agency).

If the reporting is not done within 72 hours, it shall be accompanied by the reasons for the delay.

Learning outcomes

- understand the concept of data breach
- identify obligations in case of personal data breach
- describe the data breach procedure

After watching the short educational video, there are 7 lessons that need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

The practical part of the "Personal Data Breaches" course consists of an online form with **15 questions** that you fill in in the event of a personal data breach in your organisation in order to decide whether or not to notify the supervisory authority (AZOP) and the data subjects of the breach. Based on your answers, Olivia will generate a report with a risk assessment **(low, medium, high, very high)** in case of high/very high risk to the respondent by instructing them to report the violation to the Personal Data Protection Agency and to the respondents.

The questionnaire is predominantly based on **the ENISA** methodology and the following factors shall be taken into account in the risk assessment:

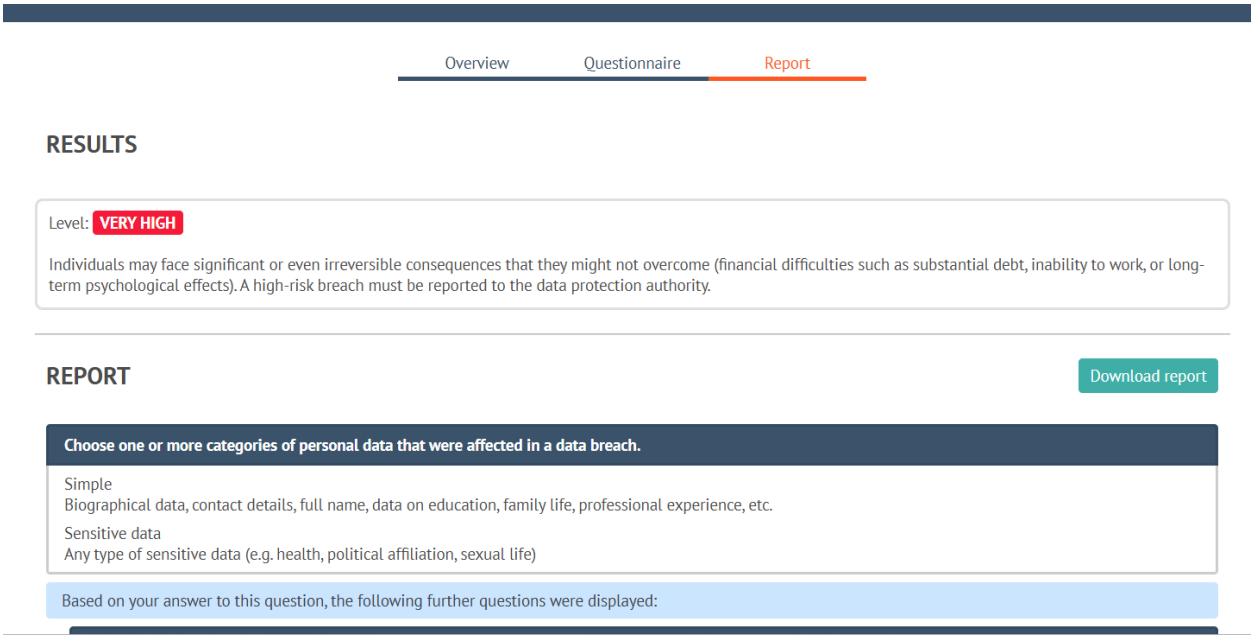
- type of infringement
- nature, sensitivity and volume of data;
- the ease of identifying an individual,
- the seriousness of the consequences for individuals;
- the specific characteristics of the individual and the specific characteristics of the controller;
- Number of individuals affected

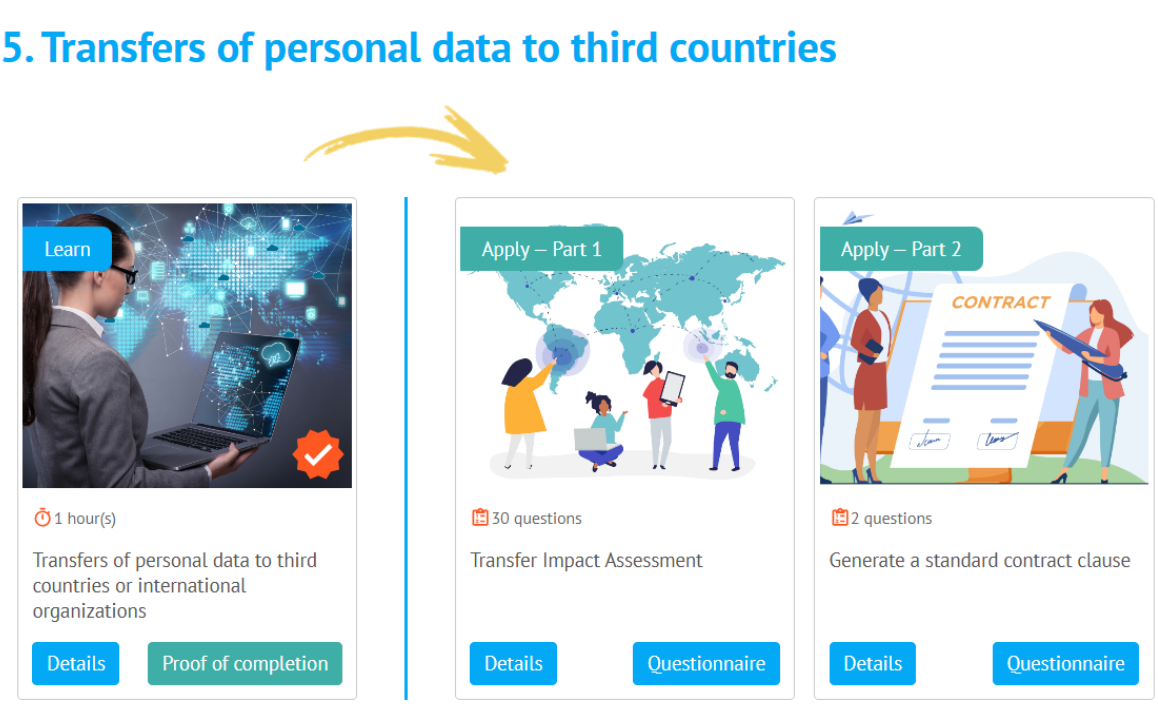
Potential risk is categorised into four categories: low, medium, high and very high.

We point out that the questionnaire is purely informative, i.e. an auxiliary tool when deciding whether it is necessary to report the violation to the data protection authority. Completing this questionnaire does not constitute an official notification of a personal data breach to the data protection authority.

By clicking on the **"DOWNLOAD REPORT"** button, you can download the questionnaire with your answers in .pdf format.

The user has the possibility to fill in a new questionnaire for each data breach. Your filled questionnaires are not saved within the user interface, but you have the option to export and save each completed questionnaire to your computer. After that, if necessary, you can fill out a new one for a new data breach.





In the theoretical module **of the course "Transfers of personal data to third countries",** users can learn what transfers of personal data to third countries are. Transfers of personal data between the EU/European

Economic Area (EEA) and third countries are indispensable for international trade and international cooperation. When personal data is transferred or made available to entities outside the territory of the EU or the EEA or to international organisations, the conditions laid down in Chapter V of the GDPR apply. The overarching purpose of Chapter V is to provide individuals whose personal data is transferred to third countries with the same level of protection of their personal data as guaranteed by the GDPR.

The aim of the module is to teach users how to recognize that in their business they transfer personal data to third countries and how to align these transfers with legal obligations under the General Data Protection Regulation.

Learning outcomes

- Understand the key principles and concepts of data transfer under the General Data Protection Regulation (GDPR)
- Assess the adequacy of data protection measures in third countries or international organisations to ensure compliance with the GDPR
- Apply appropriate safeguards and mechanisms for the transfer of personal data outside the European Economic Area (EEA) in accordance with the requirements of the GDPR
- Assess the potential risks associated with the transfer of personal data to third countries
- Understand the rights of data subjects in relation to international data transfers and the mechanisms available for exercising these rights.

After watching the short educational video, there are **7 lessons that** need to be studied in detail to master the material, and after that we advise you to approach the knowledge test.

If you have more than 80% correct answers, Olivia will generate a certificate of successful completion of the module.

The practical part of **the course "Transfers of personal data to third countries"** consists of 2 online forms (questionnaires):

- online questionnaire for conducting an analysis of the impact of the transfer of personal data on data subjects (TRANSFER IMPACT ASSESSMENT -TIA).

The purpose of this practical module is to help entrepreneurs who export personal data to a third country to carry out an analysis of the impact of the transfer of personal data to third countries.

After answering the questions from the online form (questionnaire), Olivia will generate a document template that you can download as a Word document to your computer and further edit as needed. Also, it is possible to modify the answers to the questionnaire in Olivia, and re-perform a new assessment.

- online questionnaire for the generation of standard contractual clauses

The first thing to check when transferring personal data to a third country is whether there is an adequacy decision for the third country to which you want to transfer personal data. In the absence of an adequacy decision, for most organisations, the most relevant instrument for the transfer of personal data from the EU to non-EU entities or international organisations is **the standard contractual clauses**.

This generator generates only standard contractual clauses for the transfer of personal data to third countries in accordance with the European Commission Implementing Decision EU 2021/914 of 4 June 2021 in the Italian language for which Italian law is applicable and for which the Garante Privacy is responsible.

It is necessary to choose one of the 4 options that suit your particular situation, i.e. the role in the personal data processing activity (whether the controller transferring personal data to another controller, the controller transferring personal data to a processor or the processor transferring personal data to a controller in a third country).

Once the Word document is generated, the text needs to be checked, the parts of the text marked with dots need to be completed, and the information needs to be filled in by the contracting parties (exporter and data importer). The wording of the clauses is not allowed to change in the main parts, but the parties may agree on certain deadlines, technical and organisational measures, additional obligations, the possibility and method of contracting the sub-processor, the applicable law and the competent supervisory authority.

Finally, upon successfully completing all 15 knowledge tests, Olivia will issue a certificate confirming your successful completion of all courses!

Congratulations!

Proofs of course completion

Achieved proofs

All courses completed!		Download
What I need to know about GDPR?	Go to course	Download
What is a privacy policy and why should you have one?	Go to course	Download
Under what conditions can I use cookies on the website?	Go to course	Download
What are data breaches and what should be done in the event of a breach?	Go to course	Download
Who is the data protection officer and what are his tasks?	Go to course	Download
Technical measures for the protection of personal data	Go to course	Download
What are the legal bases for processing personal data?	Go to course	Download