

## 15 COURSES (PRACTICAL AND THEORETICAL MODULES)

- 1) General Data Protection Regulation - basics
- 2) Principles of data protection
- 3) Legal bases for processing personal data
- 4) Privacy policy
- 5) Data protection officer
- 6) Data protection impact assessment
- 7) Records of processing activities
- 8) Agreement between the data controller and data processor
- 9) Organizational measures
- 10) Technical measures
- 11) Video surveillance
- 12) Cookies
- 13) Rights of the data subject
- 14) Transfers of personal data to third countries
- 15) Data breaches



**ARC2 Project for SMEs: Introducing Olivia - Your Simplified Solution for GDPR Compliance**

## WHAT IS ARC II PROJECT AND WHAT DO SMEs need it?

- ✓ Small and medium-sized enterprises (SMEs) play a key role in the European economy. These enterprises are often described as the backbone of the economy as they constitute the majority of businesses in Europe (more than 95% of all enterprises in EU are SMEs)
- ✓ In order to support SMEs, the European Union continuously implements various initiative aimed at strengthening the capacities of small businesses and promoting their growth and competitive position
- ✓ **The goal of the EU co-funded ARC2 project is to facilitate SMEs in complying with the General Data Protection Regulation, reduce administrative burden and financial costs, and help them realize that aligning with data protection regulations will enhance their business operations and enable them to build a relationship of trust with their customers/clients**
- ✓ Despite more than six years since its enforcement, many SMEs continue to struggle with GDPR compliance, and there is a pressing need for the development of practical guidance and digital tools that can be easily replicated in other Member States, tailored to meet the specific needs of SMEs and streamline their implementation of GDPR obligations

✓ **ARC 2 Consortium** comprised of Croatian Data Protection Authority, Italian Data Protection Authority, Faculty of Organisation and Informatics, Croatia, Vrije University Bruxelles, University of Florence decided to address the needs of the Croatian and Italian SME in relation to GDPR compliance by:

**1) Creating "Olivia," an open-source, freely accessible, interoperable, and innovative digital tool tailor-made to the needs of Croatian and Italian SMEs**

**2) Hosting 20 GDPR workshops in Croatia and 20 in Italy where SMEs can receive hands-on assistance to address their individual GDPR compliance challenges**

**3) Launching an awareness campaign in Croatian and Italian media targeting SMEs and the general public, alongside the development of educational materials and 10 informative videos**

**4) Organizing 2 validation workshops**

**5) Hosting 2 international conferences in Zagreb and Rome to disseminate the project's outcomes**

**6) Running a social media campaign to promote the digital tool Olivia and encourage its adoption by SMEs**

**7) Drafting a Handbook on personal data protection tailored for SMEs**



- ✓ The main output of ARC II project is **open-source, interoperable web tool Olivia, easy to use and free of charge, aimed to help SMEs to comply with GDPR and national Croatian and Italian data protection legal framework**
- ✓ The main objective of the Olivia web tool is providing practical support to Croatian and Italian SMEs in the implementation of the data protection legislation (GDPR, but also Italian and Croatian national legislation) and principles in the day to- day business activities
- ✓ **Olivia offers 15 data protection courses that encompass all key responsibilities for data controllers/processors outlined in the GDPR. Each course includes both theoretical and practical modules**
- ✓ In theoretical part SMEs can go through lessons to learn about the specific obligation from the GDPR, they can watch educational video and afterwards they can take a test to test their knowledge
- ✓ After watching a video and reading the short educational materials, the user will need to fill out the questionnaire (quiz) regarding topic in question to test his/her knowledge. After the successful completion of the questionnaire (at least 80% correct answers), the user will receive a certificate as a proof of completion of certain theoretical module
- ✓ In the practical part, SMEs have the ability to create essential "GDPR documents" that can assist them in demonstrating their compliance or evaluating the level of compliance within their organization

**15 courses** on following topics:

**1) GDPR basics**

**2) Data protection principles**

**3) Lawful basis for processing of personal data**

**4) Privacy policy/notice**

**5) Data protection officer**

**6) Data protection impact assessment**

**7) Records of processing activities**

**8) Contract between data controller and data processor**

**9) Organisational measures**

**10) Technical measures**

**11) Video Surveillance**

**12) Cookies and other tracking technologies**

**13) Data subject rights**

**14) Data transfers**

**15) Data breaches**

**In addition, OLIVIA CONTAINS 20 WEBINARS IN ITALIAN AND CROATIAN ON VARIOUS DATA PROTECTION TOPICS - permanently available in Olivia web tool, available free of charge to all the interested stakeholders**

## GDPR topics

### GDPR topics – Learn and Apply

Olivia is a virtual teacher and assistant at the same time. Olivia contains a small online academy that offers you a series of learning modules to improve your knowledge in the field of personal data protection, and also serves as a practical tool to help you create internal documents to prove your compliance and reliability.



General Data Protection Regulation (GDPR) Basics

Show



Principles of personal data processing

Show



Legal Basis for Data Processing

Show



Privacy Policy/Notice/Statement

Show



Rights of the data subject

Show



The relationship between data controller and data processor

Show



Records of Processing Activities

Show



Organizational measures for personal data protection

Show



Rights of the data subject

Show



The relationship between data controller and data processor

Show



Records of Processing Activities

Show



Organizational measures for personal data protection

Show



Technical Measures

Show



Data protection impact assessment

Show



Data Protection Officer (DPO)

Show



Cookies

Show



Video surveillance and processing of personal data

Show



Data Breach

Show



Transfers of personal data

Show





Co-funded by the European Union



Croatian Personal Data Protection Agency  
**azdp**  
Agencija za zaštitu osobnih podataka

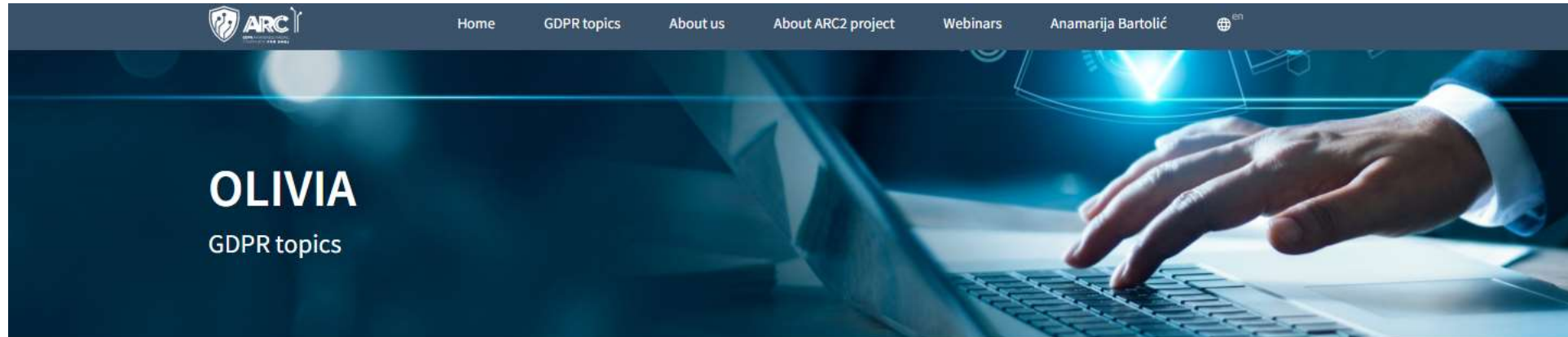


**GDPR**

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



GDPR AWARENESS RAISING CAMPAIGN FOR SMEs



### General Data Protection Regulation (GDPR) Basics

**Theoretical module**

Learn



1 hour(s)

What I need to know about GDPR?

Details Certificate



Apply — Part 1




17 questions

Assess the level of compliance in your organization/company

Details Questionnaire

Apply — Part 2



52 questions

Checklist to verify the state of compliance with the GDPR

Details Questionnaire

**Practical modules**

**About topic**

In this sub-module, small and medium-sized enterprises (users) user will be able to learn and understand the main terminology of the General Data Protection Regulation (GDPR): what is the protection of personal data; what is the role of the supervisory authority; scope of the GDPR; who is the data subject; what are personal data; what are the special categories of personal data; what is the processing of personal data; what is the difference between controllers, processors and joint controllers; what is the objective of the GDPR and data protection regulations, why data protection is important, both for individuals and organizations, etc. After watching the video and after reading the educational materials, the users will be able to fill out the test and answer questions to check their knowledge. The user will be offered statements, in respect of which he/she will be able to state whether he/she considers them correct or incorrect. Once the user gives the answers, an explanation of the correct answer will appear. If the user achieves a minimum of 80 % correct answers, then the system will generate a certificate as proof of successfully passing the theoretical sub-module.

**Learning outcomes**

- understand the main terminology of the General Data Protection Regulation (GDPR)
- identify the special categories of personal data
- describe the objective of the GDPR and data protection regulations

**Connected practical modules**

- Personal data protection as a human right [Mark as done](#)
- About the General Data Protection Regulation (GDPR) [Mark as done](#)
- Territorial and material scope [Mark as done](#)
- Basic terminology [Mark as done](#)
- Personal data and data processing [Mark as done](#)
- Data controller [Mark as done](#)
- Joint data controllers [Mark as done](#)
- Data processor [Mark as done](#)
- Act on the implementation of the GDPR [Mark as done](#)



GDPR topics > General Data Protection Regulation (GDPR) Basics > Learn

## What I need to know about GDPR?

1 hour(s) 12 lessons 1 quiz

What I need to know about GDPR?

1 hour(s) 12 lessons 1 quiz

Overview Lessons Certificate

**List of lessons**

- Personal data protection as a human right
- About the General Data Protection Regulation (GDPR)
- Territorial and material scope
- Basic terminology
- Personal data and data processing
- Data controller
- Joint data controllers
- Data processor

1. Right to protection of personal data is a fundamental human right. The aim of protecting the right to personal data is to ensure that individuals have control over their personal data and that their personal data is processed fairly, lawfully, and securely by organizations and authorities.

True False

Overview Lessons Certificate

Overview Lessons Certificate

**List of lessons**

- Personal data protection as a human right
- About the General Data Protection Regulation (GDPR)
- Territorial and material scope
- Basic terminology
- Personal data and data processing
- Data controller

**Quiz**


This quiz contains 10 questions.

Please note that the passing score is 80% and that the results are available immediately after quiz submission. The number of submissions is not limited and the Results will display only your best score.

To start the quiz, please click the Take quiz button below.

Your grade: 100%

Take quiz Results



**List of lessons**

- Personal data protection as a human right
- About the General Data Protection Regulation (GDPR)
- Territorial and material scope
- Basic terminology
- Personal data and data processing
- Data controller



After successfully passing the test, the user will receive a detailed report containing the correct answers and explanations, along with a certificate of completion.

list of lessons

- Personal data protection as a human right  
Reading
- About the General Data Protection Regulation (GDPR)  
Reading
- Territorial and material scope  
Reading
- Basic terminology  
Reading
- Personal data and data processing  
Reading
- Data controller  
Reading
- Joint data controllers  
Reading
- Data processor  
Reading
- Act on the Implementation of the GDPR  
Reading
- Supervisory authority  
Reading

The Italian Personal Data Protection Authority (GPDP) is an independent supervisory authority, hence is not an agency that falls under the jurisdiction of a Ministry. GPDP offers advices and guidance, promotes good practices, carry out audits, consider complaints, monitors compliance with the GDPR and takes enforcement action.

**3. Personal data in accordance with the General Data Protection Regulation (GDPR) are only data that are directly linked to a particular person, such as his name, surname, personal identification number, date of birth etc. Personal data that cannot be directly be linked to a person is not data categorized as "personal".**

Correct answer: **False**  
Your answer: **False**



Personal data is any information that relates the person if the person can be identified by this information. Thus, identifiable factor can also be personal data. For example, genetic information, such as blood samples, may lead us to certain name and surname in combination of other data such as hospital's appointment number.

**4. Personal data related to ethnic origin, political opinions, religious or philosophical beliefs deserves higher level of safety.**

Correct answer: **True**  
Your answer: **True**



Personal data regarding person's race, ethnic origin, political opinion, religious/philosophical belief, trade union membership, genetic/biometric or health data, sex life or orientation are personal data of special category. If you process this type of data this means you are processing more sensitive data in their nature, and by this you have to take more safety measures because the risk of for example, non - authorized access is much higher. For example, you are a medical clinic and at the request of the patient you send medical results by an e-mail. However, the e-mail you have is not correct and you have not updated this information in such a way that before agreeing to send the results via e-mail, you asked the patient to check whether the information about his e-mail was correct. In this way, you have not taken all the safeguards to reduce the risk of unauthorized disclosure of the patient's health information and thus your company as controller is responsible for data breach. Also, there are personal data of a sensitive nature, for example data about children, the elderly, asylum seekers etc. which also deserves higher level of safety because these group of people may be less aware of the risks, consequences and safeguards of the processing of their personal data.

**5. If you replace the name or other data with certain reference number you are not processing personal data. Personal data is only the name hiding behind reference number, and this reference number is anonymized information.**

Correct answer: **False**




Congratulations, Anamarija Bartolić!

(It's the way to make it happen that efforts haven't gone unnoticed. Your effort is worthy!)

Download Certificate

CERTIFICATE OF COMPLETION



**Anamarija Bartolić**  
for  
**GDPR Basics**

**Workload:** 1 hour(s)

**Learning outcomes:**

- understand the main terminology of the General Data Protection Regulation (GDPR)
- identify the special categories of personal data
- describe the objective of the GDPR and data protection regulations

**Link:** [olivia-gdpr-arc.eu/en/course/overview/1](https://olivia-gdpr-arc.eu/en/course/overview/1)



Co-funded by  
the European Union



Croatian Personal Data Protection Agency



Agencija za zaštitu osobnih podataka



# GDPR checklist- practical module contains a form with 52 questions to assess the level of compliance within the organisation

Overview **Questionnaire**

**Personal data**

Consent based data processing (Articles 7, 8 and 9)

\* Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of statement or a clear affirmative action?

Yes  
 No

\* If personal data that you currently hold on the basis of consent does not meet the required standard under the GDPR, have you re-sought the individual's consent to ensure compliance with the GDPR?

Yes  
 No

\* Are procedures in place to demonstrate that an individual has consented to their data being processed?

Yes  
 No

\* Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?

Yes  
 No

Children's personal data (Article 8)

\* Where online services are provided to a child, are procedures in place to verify age and get consent of a parent/ legal guardian, where required?

Yes  
 No

Legitimate interest based data processing

\* If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? That analysis must demonstrate that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, 3) the processing is not prejudicial to or overridden by the rights of the individual.

Yes  
 No

[Previous](#) [Next](#)

[Save for later](#)

**Data subject rights**

Access to personal data (Article 15)

\* Is there a documented policy/procedure for handling Subject Access Requests (SARs)?

Yes  
 No

\* Is your organisation able to respond to SARs within one month?

Yes  
 No

**Data portability**

\* Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format?

Yes  
 No

Deletion and rectification (Articles 16 and 17)

\* Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?

Yes  
 No

Right to restriction of processing (Article 18)

\* Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?

Yes  
 No

Right to object to processing (Article 21)





# Questionnaire to assess the level of GDPR (personal data protection) awareness in organization/company

Overview

Questionnaire

\* 1. In my company, personal data processing takes place. We don't process personal data of clients or customers, but we process personal data of our employees.

- Yes
- No

\* 2. In our company, we process at least one of the types of personal data listed below:

- Personal data on racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data processed for the purpose of uniquely identifying a natural person
- Health data
- Data on a natural person's sexual life or sexual orientation

- Yes
- No

\* 3. Do you process the personal data of any of the following persons: client, user, customer, party, supplier, worker, website visitor etc.?

- Yes
- No

\* 4. In our company we process personal data of "vulnerable groups", such as children, elderly people, asylum seekers, patients, etc.

- Yes
- No

\* 5. We process personal data fairly in our company, and all employees understand how we do this.

- Yes
- No

\* 6. I am familiar with the laws governing the business activity of the organisation/company.

For example, if the company is a hotel, I am familiar with the Law on the Provision of Tourist Services; if the company is engaged in the sale of certain products, I am familiar with the Civil Obligations Act, etc.

Do you recognise any of these patterns in your activities?

- Yes
- No

\* 13. In our business, in most cases, we determine the reason why a certain data processing will be carried out (we determine the purpose of data processing not some other company).

- Yes
- No

\* 14. Regarding the cooperation of the organisation/company with other legal entities, does the organisation/company know how to properly define its role?  
For example, the organisation/company has engaged another business entity to store personal data that processes personal data in the cloud. Do you know if your organisation/company is a controller or processor in this case?

- Yes
- No

\* 15. If the organization/company has a relationship between the controller and the processor, your organization/company include optional provisions in the data processing contract.

- Yes
- No

\* 16. Although my company may identify itself as a data processor, it still makes decisions on certain aspects of the data processing process.

- Yes
- No

\* 17. Do you make decisions together with another organisation/company on specific data processing operations?

- Yes
- No

Submit



# Questionnaire to assess the level of GDPR (personal data protection) awareness in your organization/company – Olivia generates the report with explanations



## 9. I am well-informed about how long personal data that we process in our company should be kept.

No

**Description:**

Check out all the regulations that regulate your business and business activities you are engaged in.

Often, special regulations determine the storage time for a particular processing of personal data.

According to accounting regulations, workers' salaries and an analytical record of salaries for which compulsory contributions are paid are kept for a certain number of years depending on national law, so, for example, personal data contained in the accounting records are subject to a 10-year retention obligation.

If you have checked the specific regulations governing your business activity and the retention period is not specified, this means that the legislator cannot predict in advance how long you will need some personal data.

This is something organisations/companies should know. In this case, consider the time frame needed to obtain this information and set it according to your internal rules.

Set a time limit that you can justify and argue. Check the personal information you hold from time to time. If you no longer need it, either delete it, or anonymize it.

Please note that personal data may only be stored for longer if necessary for archiving, scientific or historical research purposes or statistical purposes.

For example, if you need to keep some personal information about your client in order to resolve any complaints, this may be considered a justified reason for storing the user's data.

## 11. Persons whose personal data are processed by the organisation/company in which I work are aware that the organisation/company processes their personal data.

No

**Description:**

The organisation/company must be transparent towards the persons whose personal data it processes.

Customers, users, workers, third parties and all persons whose personal data are processed should be informed about who the controller is and why and how personal data are processed.

It is very important to point out that the language used by the organisation/society must be simple, clear and tailored to the persons whose personal data it processes. This should be taken into account in particular where personal data of "vulnerable groups" such as personal data of children or the elderly are processed.

Familiarise people with the processing of personal data in your organization/company for example by providing layered privacy notices on the site. If you do not have a website, you can put information about the processing of personal data in a visible place (e.g. on a notice board or stand in the waiting room).

The Privacy Policy template can be found here: ....

OLIVIA  
GDPR topics

Home | GDPR topics | About us | About ARC2 project | Webinars | Anamarija Bartolić

GDPR topics > Privacy Policy/Notice/Statement > Learn

## What is a privacy policy and why should you have one?

2 hour(s) | 5 lessons | 1 quiz

Overview | **Lessons** | Certificate

Privacy Policy/Notice/Statement

2 hour(s)

What is a privacy policy and why should you have one?

Details | Certificate

44 questions

Create your own privacy policy

Details | Report

List of lessons

- Introduction  
Reading
- Content of the privacy policy  
Reading
- Compatibility with the GDPR  
Reading
- Informing individuals on processing personal data  
Reading
- FAQ  
Reading
- Quiz  
Quiz

Informing individuals on processing personal data

Mark as done

**How should small and medium-sized enterprises inform individuals about the processing of their personal data and their rights?**

Typically, all this information is provided to individuals in a separate document, often referred to as a Data Processing Notice/Privacy Notice/Privacy Policy/Privacy Statement/Privacy Statement. A separate document means that this information should not be contained in or is a part of another document (e.g., to form part of the terms of use, contractual terms, or general conditions).

If your organization/company has a website, you should publish such a document on the website, where this is visible, so that individuals can easily find and inform themselves about how you process their data (it is advisable to place a link to the document in question at the foot of the website or website header, on the main page and on all other pages).

It is up to you to determine the specific way (format/modality) through which you will fulfil your legal obligations to inform data subjects (your clients, employees, associates, etc.) about their rights and the processing of personal data. Please note that the name of the document is not strictly defined nor does the GDPR prescribe where you must publish it, **but it is important that it is clearly visible to individuals and easily found!**

It is also important to stress that this document must consist of all the elements required by the provision of Article 13 of the GDPR.

**What does "easily available" mean?**

"Easily available" means that an individual should not seek information; it should be immediately clear where and how this information can be accessed (e.g., by sending it directly (i.e., by e-mail), connect to it, publish it in a visible place on the website, use a layered online privacy statement/notice, frequently asked questions, pop-ups, etc.).

**What is a layered policy/notice/privacy statement?**



GDPR topics > Privacy Policy/Notice/Statement > Learn

## What is a privacy policy and why should you have one?

2 hour(s) 5 lessons 1 quiz

Overview Lessons Certificate

### List of lessons

- Introduction Reading
- Content of the privacy policy Reading
- Compatibility with the GDPR Reading
- Informing individuals on processing personal data Reading
- FAQ Reading
- Quiz Quiz

### Quiz results

**1. The privacy policy/statement/notice on the processing of personal data is an internal statement governing the organization's handling of personal data. It is intended for organizations/companies and their employees who process personal data to give them instructions on how to protect them.**

Correct answer: False  
Your answer: False

While every organization/company (data controller) needs to establish internal policies governing the handling of personal data within an organization/company, the privacy policy to which we refer applies to individuals whose personal data is processed in order to inform them of what happens to their data and their rights.

**2. The aim of the privacy policy is to inform data subjects about their data protection rights and how data controllers (small and medium-sized enterprises – organizations/companies) use their data. It is important that each data controller (small and medium-sized enterprise – organizations/companies) is transparent about how it uses the personal data of its employees and customers, as people have the right to know them, and this is a key requirement of the General Data Protection Regulation (GDPR) (principle).**

Correct answer: True  
Your answer: False

Yes, the right to information is the practical implementation of the fundamental principles of the processing of personal data in line with the GDPR – the principles of legality, fairness, and transparency. Every data subject shall have the right to obtain from the controller (small and medium-sized enterprise) any information referred to in Article 13 of the GDPR.

**3. In privacy policy, organizations/companies should explain to individuals in a very complex, unclear and general way what they do with their personal data.**

Correct answer: False  
Your answer: False

Home GDPR topics About us About ARC2 project Webinars Anamarija Bartolić

GDPR topics > Privacy Policy/Notice/Statement > Apply

## Create your own privacy policy

Overview Questionnaire Report

### Tell individuals which type of data you are processing

Explanation: In this section, it is necessary to inform the individuals about the type of personal data that you have collected/stored/delivered /recorded/structured, or otherwise processed. Each organisation processes different types of data, so in this section, you need to indicate which personal data you process.

#### Personal identifiers (common personal data)

- Name and surname
- E-mail address
- Date of birth
- Home address
- Age of the individual
- Gender
- Marital status
- IP address or domain name of the computer through which individuals visited your website
- Location data (i.e. GPS)
- Photographs (displaying individuals)
- Video records
- Audio records
- Vehicle registration number

Add

Personal data perceived as sensitive data

## Create your own privacy policy

Overview **Questionnaire** Report

### Tell individuals why you process their personal data (purpose of processing), state the legal basis for the processing and time period of data storage

Explanation: it is necessary to adapt this section to purposes for processing in your organisation. Here are some examples: "In order to make a reservation of hotel accommodation, we collect your personal data: name, and surname, credit card numbers and we keep it for one month." "For the purposes of concluding the sales contract, we collect your personal data: name, surname, address, ID number which we keep for 2 years." "For the purpose of protecting the property XX, we collect data through a video surveillance system based on a legitimate interest, and we keep the records for 1 month." "If it is a matter of processing personal data based on a legal or contractual obligation or is a condition necessary for concluding a contract, you must inform the individual whether he/she has an obligation to provide personal data and what are the possible consequences if such data is not provided." "The time period for storage of personal data is frequently prescribed by laws that regulate your business. For example, lawyers are obligated to keep files for the time period prescribed by the law which regulates the legal profession." "If not specified, be guided by the principle of "storage limitation" which stipulates that personal data shall be kept for as long as necessary for the purposes for which the personal data are processed, and may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes." "You need to know how long it is necessary to store personal data for the purposes for which you are processing personal data, if possible, specify the criteria by which you set the storage period." "Also, when it comes to data that you did not collect directly from the individual (for example, in kindergarten you collect personal data from parents about persons who are allowed to pick up their child from kindergarten) be sure to indicate the source of this data."

Choose all that apply. For some choices you will have to provide information on legitimate reasons, legal bases, and retention periods.

- For the purposes of concluding the sales contract, we process your data (\_\_\_\_ [enter type of data]) which we will keep for \_\_\_\_ [enter how long you will keep it].
- Without the processing of your personal data, we are not able to conclude a contract with you.
- For the purposes of the employment contract, we process your data (\_\_\_\_ [enter type of data]) which we will keep for \_\_\_\_ [enter how long you will keep it].
- We process your personal data (\_\_\_\_ [enter type of data]) in order to fulfill legal obligations in accordance with regulation which we will keep for \_\_\_\_ [enter how long you will keep it].
- Based on our legitimate interest, we process your personal data (\_\_\_\_ [enter type of data]) which we will keep for \_\_\_\_ [enter how long you will keep it].
- We are processing your personal data (\_\_\_\_ [enter type of data]) because we have a vital interest and we will keep it for \_\_\_\_ [enter how long you will keep it].
- We process your personal data (\_\_\_\_ [enter type of data]) based on your consent and we will keep it for \_\_\_\_ [enter how long you will keep it].
- We are processing your personal data (\_\_\_\_ [enter type of data]) to perform a public task we will keep it for \_\_\_\_ [enter how long you will keep it].
- In most cases, the personal data we process is given to us directly by individuals, but we also process the personal data that we collect indirectly, meaning from other sources.
- We collect personal data from \_\_\_\_ [enter the source of your data] in order to \_\_\_\_ [enter the purpose of collecting data].
- After we no longer need your data we will securely destroy or dispose of your data: \_\_\_\_ [explain how you will dispose of their data]. We will delete your data or anonymize it.

Enter the type of data for the following statement: (1)

For the purposes of concluding the sales contract, we process your data (\_\_\_\_ [enter type of data]) which we will keep for \_\_\_\_ [enter how long you will keep it].

+ Add

name, surname and date of b

\* Enter the data retention period for the following statement: (1)

For the purposes of concluding the sales contract, we process your data (\_\_\_\_ [enter type of data]) which we will keep for \_\_\_\_ [enter how long you will keep it].

1 year.

Enter the type of data for the following statement: (2)

For the purposes of the employment contract, we process your data (\_\_\_\_ [enter type of data]) which we will keep for \_\_\_\_ [enter how long you will keep it].

+ Add

name, surname, date of birth

GDPR topics > Privacy Policy/Notice/Statement > Apply

## Create your own privacy policy

Overview **Questionnaire** Report

### Inform individuals about their rights

Explanation: individuals have the right to information, access, rectification, erasure, restriction of processing, data portability, and the right not to be subjected to automated individual decision making including profiling. Explain to individuals that their rights are not absolute and the rights differ depending on the lawful basis for processing. For example, if the processing is not based on a contract/consent or the portability of the data is technically unfeasible, there is no obligation to fulfill the right to data portability. Describe to individuals how they can exercise their rights.

Describe to individuals how they can exercise their rights.

Select everything that applies:

- Your right of access
  - You have the right to request information about the processing of your personal data: what personal data we process, the purposes of processing, with which we share, etc., and request copies of your personal data.
- Your right to rectification
  - You have the right to rectify your personal data that is inaccurate.
- Your right to erasure
  - In some circumstances you have the right to delete your personal data. For example, we cannot delete your data if we are legally obliged to keep it for a predetermined period of time.
- Your right to restriction of processing
  - In certain circumstances you have the right to ask us to restrict the processing of your personal data.
- Your right to object to processing
  - In certain circumstances, you have the right to object to the processing of your personal data.
- Your right to data portability
  - You have the right to request that we transfer the personal data you have provided to another organization or to you, if the processing is based on a contract/consent.

Enter contact information which an individual can use to exercise their rights.

E-mail address:  
dpo@popatija.hr

Phone number:  
098675580

Postal address:  
Remete 77

Previous

Next

Save for later

Tell individuals which measures you have undertaken to keep their personal data safe

Explanation: Describe to individuals (as much as possible in order not to jeopardize your own security processes) your security (technical and organizational) measures.

\* [Choose "Yes" if it applies]  
We have implemented strict security measures to reduce the risk of a data breach and misuse of your personal data, such as unauthorized disclosure and unauthorized access to your data.

- Yes
- No

\* [Choose "Yes" if it applies]  
The equipment/premises on which we store personal data is located in a secure environment with limited physical access (i.e. locked room).

- Yes
- No

\* [Choose "Yes" if it applies. Choosing "Yes" will prompt you to select the measures you are applying.]  
We use firewall, strong passwords, antivirus programs and other measures to protect personal data (such as encryption and pseudonymization).

- Yes
- No

Continuing with the previous question, which measures are you applying to protect personal data?

- firewall
- strong passwords
- antivirus programs

Add

\* [Choose "Yes" if it applies]  
Only authorized person has access to personal data, and the subject matter we have regulated with our bylaws.

- Yes
- No

\* [Choose "Yes" if it applies]  
We regularly organize trainings on personal data protection for our employees to keep them informed about their obligations arising from the data protection legal framework and to raise awareness on personal data protection in our organization.

- Yes
- No

\* Are there other measures you have undertaken to keep their personal safe, which aren't mentioned in previous questions?

- Yes
- No

Inform individuals about recipients of data/categories of recipients, data transfers to third countries and international organizations, and automated decision-making involving profiling, if applicable

Explanation: You need to inform individuals about the recipients/categories of data recipients and about data transfers to third countries/international organizations in case you perform such processing. If you carry out automated individual decision-making (making a decision solely by automated means without any human involvement), which includes profiling, it is necessary to provide meaningful information about the logic of this type of processing, as well as the importance and anticipated consequences of such processing for the individual.

Select the recipients with whom you share user data with in order to provide the same users with your services:

- IT services
- Cloud services
- Payment service providers
- Delivery companies
- Website hosts

Marketing agencies

Add

Select statements that apply to your company. Some statements will open questions to enter additional information.

- We may disclose your personal to third parties such as fraud prevention bodies and law enforcement bodies to respect our legal obligations.
- We have identified lawful bases for disclosing your personal data to the abovementioned third parties and we have put in place agreements with our vendors (data processors) which regulate the processing of your personal data (according to Article 28 of the GDPR).
- We use service providers (\_\_\_\_ [enter what kind of service providers]) and we transfer your data outside of EEA to \_\_\_\_ [enter the name of the country] for the purposes \_\_\_\_ [enter purposes].
- When we transfer your personal data outside of EEA, we undertake all necessary steps and additional safeguards to ensure that the level of protection of your data and rights is the same as in the EEA.
- We carry out automated individual decision-making for the purposes \_\_\_\_ [enter purposes] and based on \_\_\_\_ [enter lawful basis].
- We implement suitable measures to safeguard your rights and freedoms and you have the right to obtain human intervention, express your point of view, and contest the decision. If you want to exercise the rights concerning automated individual decision-making, you can contact us: \_\_\_\_ [enter contact details].

Previous

Next



**Olivia automatically generates a customized privacy policy in a Word document based on the information provided by the user in the template form.**

## Privacy Policy/Statement on the processing of Personal Data

### 1. INFORMATION ABOUT THE DATA CONTROLLER

Hotel Opatija

Address: Remete 77

Phone number: 098764980

E-mail: hotel@opatija.hr

Data protection officer: dpo@opatija.hr

### 2. CATEGORIES AND TYPES OF PERSONAL DATA WE PROCESS

We collect and process the following personal identifiers (common personal data):

- Name and surname
- E-mail address
- Date of birth
- Home address
- Age of the individual
- Gender
- Marital status
- Photographs (displaying individuals)
- Video records

of arrival, date of departure.) in order to fulfill legal obligations in accordance with regulation which we will keep for 11 years..

Without the processing of your personal data, we are not able to conclude a contract with you.

### 4. TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

We have implemented strict security measures to reduce the risk of a data breach and misuse of your personal data, such as unauthorized disclosure and unauthorized access to your data.

The equipment/premises on which we store personal data is located in a secure environment with limited physical access (i.e. locked room).

We use firewall, strong passwords, antivirus programs and other measures to protect personal data (such as encryption and pseudonymization).

Only authorized person has access to personal data, and the subject matter we have regulated with our bylaws.

We regularly organize trainings on personal data protection for our employees to keep them informed about their obligations arising from the data protection legal framework and to raise awareness on personal data protection in our organization.

#### Your right to object to processing

In certain circumstances, you have the right to object to the processing of your personal data.

#### Your right to data portability

You have the right to request that we transfer the personal data you have provided to another organization or to you, if the processing is based on a contract/consent.

If the processing of personal data is based on consent, you can withdraw it at anytime. For withdrawing [consent](#) you can contact us on: [dpo@opatija.hr](mailto:dpo@opatija.hr), 098675980, Remete 77

You can exercise your rights for free. We will respond to your request in one month.

#### 6. DATA RECIPIENTS/RECIPIENT CATEGORY, DATA TRANSFER TO THIRD COUNTRIES AND AUTOMATED DECISION MAKING

We share personal data with third-party vendors and other service providers who perform functions or services on our behalf and under our instructions to make our services available to you. This includes:

- IT services
- Cloud services
- Payment service providers
- Delivery companies
- Website hosts

We may disclose your personal to third parties such as fraud prevention bodies and law enforcement bodies to respect our legal obligations.

#### 8. THE RIGHT TO SUBMIT A COMPLAINT REGARDING THE PROCESSING OF YOUR PERSONAL DATA

If you have any concerns or remarks about how we use your personal data, you can complain to us at [dpo@opatija.hr](mailto:dpo@opatija.hr).

You can also file a complaint to the supervisory authority:  
Croatian Personal Data Protection Agency, Selska cesta 136, Zagreb, email: [azop@azop.hr](mailto:azop@azop.hr)

#### 9. PRIVACY POLICY CHANGES

We regularly update the privacy policy so that it is accurate and up-to-date, and we reserve the right to change its content if we deem it necessary. You will be informed about all changes and additions in a timely manner through our website in accordance with the principle of transparency.

Last update: 08.06.2024.



## Video surveillance and processing of personal data



2 hour(s)

Video surveillance and processing of personal data

Details

Certificate



8 questions

Create a notice on the processing of personal data through the video surveillance system

Details

Report



13 questions

Create Policy on video surveillance

Details

Report

**Theoretical module and two practical modules: Create a video surveillance notice and Create a policy on video surveillance**

Home | GDPR topics | About us | About ARC2 project | Webinars | Anamarija Bartolić

GDPR topics > Video surveillance and processing of personal data > Learn

### Video surveillance and processing of personal data

2 hour(s) | 10 lessons | 1 quiz

Overview | Lessons | Certificate

- Legal bases for processing personal data through video surveillance
- Legality of video surveillance use; identification of legal basis and lawful purposes.
- Workplace video surveillance:
- Notice that the premises are under video surveillance
- A policy on video surveillance:
- Who has the right to access video surveillance recordings?
- Retention period of video surveillance recordings
- Legality of processing
- Systems for monitoring and control of company vehicles
- Processing of biometric personal data in the private sector
- Quiz

- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Mark as done
- Passed

**Provisions on video surveillance (Articles 25-32 of the Croatian Act on Implementation of the GDPR)**



Home GDPR topics About us About ARC2 project Webinars Anamarija Bartolić

GDPR topics > Video surveillance and processing of personal data > Apply

### Create a notice on the processing of personal data through the video surveillance system

Overview **Questionnaire**

\* Enter the name of the controller (company/organization name).

Hotel Opatija

\* Enter the contact information through which the respondents can exercise their rights.

dpo@opatija.com

\* Enter the legal basis on which you process personal data via video surveillance.

legitimate interest

\* Enter the recording retention period.

2 months

\* Where can the respondent find complete information about the processing of personal data by the controller?

On the website  
 In our office  
 Elsewhere

\* Enter a link to the website where the respondent can find complete information about the processing of personal data by the controller, i.e. a link to the Privacy Policy.

Olivia generates a video surveillance notice based on the responses provided in the form.



**THE PREMISES ARE UNDER VIDEO SURVEILLANCE**

**DATA CONTROLLER:** Hotel Opatija

**CONTACT INFO:** dpo@opatija.com

**Purpose of processing:** protection of people and property

**Legal basis:** legitimate interest

**Recording retention period:** 2 months

**Respondents' rights** (of natural people recorded by video surveillance cameras): The right to access your personal data, the right to delete them, the right to limit their processing, and the right to object to their processing

**Complete information on the processing of your personal data** by the controller can be found in the *Privacy Policy* available on website opatija@hotels.com

# OLIVIA

GDPR topics



After reading educational materials and watching video, user can take a quiz to test its knowledge

## Legal Basis for Data Processing

Learn

2 hour(s)

What are the legal bases for processing personal data?

Details Certificate

Apply — Part 1

28 questions

Determine the legal basis for processing personal data

Details Questionnaire

Apply — Part 2

12 questions

Consent for personal data processing

Details Questionnaire

Apply — Part 3

GDPR topics > Legal Basis for Data Processing > Learn

What are the legal bases for processing personal data?

2 hour(s) 4 lessons 1 quiz

### List of lessons

- Introduction
- Legal basis for data processing
- Consent as a legal basis for data processing
- Contract as a legal basis for data processing
- Legal obligation as a legal basis for data processing
- The vital interests of the individual as a legal basis for data processing
- Public task as a legal basis for data processing
- Legitimate interest as a legal basis for data processing
- video

3. In our organization/company, we take care of compliance with various laws, including compliance with the GDPR. That is why we have adopted the Rules on the processing of personal data, where we have laid down certain obligations regarding the processing of personal data in our organization/company. In this way, the organization/company has a legal obligation as a legal basis for the processing of personal data.

True False

Course Legal Basis for processing of personal data consists of theoretical part (module) and practical part (3 modules)





Co-funded by  
the European Union



Croatian Personal Data Protection Agency  
**azDP**  
Agencija za zaštitu osobnih podataka



**GDPR**

GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI



## List of lessons

- Introduction  
Reading
- Legal basis for data processing  
Reading
- Consent as a legal basis for data processing  
Reading
- Contract as a legal basis for data processing  
Reading
- Legal obligation as a legal basis for data processing  
Reading
- The vital interests of the individual as a legal basis for data processing  
Reading
- Public task as a legal basis for data processing  
Reading
- Legitimate interest as a legal basis for data processing  
Reading
- Video  
Video
- Quiz  
Quiz

The legal obligation must be imposed exclusively by the law or by the bylaws published in the official journal in which the regulations are published (e.g., the Official Gazette).

It is not possible to impose obligations with internal rules and hope it can pass as a legal obligation.

Think about it a little bit.

If that were the case, there would be no need for consent, contract or legitimate interest, but the organization/company would only prescribe a legal obligation it wants and, consequently, do what it wishes with personal data.

Looks like that's not, right?

**4. An organization/company may rely on a contract as a legal basis for the processing of personal data where a contract with an individual exists and the organization/company must process the personal data of the opposing party in order to fulfil its obligations under the contract.**

Correct answer: **True**  
Your answer: **True**



Organizations/companies enter different contracts. For example, a contract with service providers. Certain personal data (e.g., first name, surname, personal identification number, address, registration number, etc.) of an individual who contracts a car insurance service are necessary for the performance of the contract, therefore the contract may constitute a legal basis for the processing of the individual's personal data.

**5. An individual has requested an offer from an organization/company because they want to purchase a service. It is necessary to process certain personal data of clients. However, such processing cannot be based on a contract but could be based on a legitimate interest.**

Correct answer: **False**  
Your answer: **False**



The processing of personal data is based on a contract even if the acts necessary for the conclusion and performance of that contract are taken. For example, when pre-contracting, bidding, etc.

This applies even if the potential client does not enter a contract with the organization/company, provided that the processing was in the context of a potential contract with that client.

**6. The general terms and conditions are a contract. The organization/company has stipulated in the general terms and conditions that the processing of personal data is necessary to improve our service (purpose). In this way, we have "covered" all possible processing of personal data and do not expect any unpleasant surprises because our clients have agreed to such a contract.**

Correct answer: **False**  
Your answer: **False**



It is true that the person whose personal data is processed must be a party to the contract, however, the personal data must be necessary for the performance of that contract. Where personal data are not necessary for the performance of a contract,

After taking quiz, Olivia will generate the report with correct answers and explanations.

**8. The General Data Protection Regulation (GDPR) sets very high standards for consent. Consent means to offer individuals real choice and control over their personal data, meaning that they are informed of your intentions and have the right to decide whether they consent to what you intend to do with their personal data.**

Correct answer: **True**  
Your answer: **True**



Consent must meet all the requirements of the GDPR. It must be freely given, informed, unambiguous and the data subject must be able to withdraw consent at any time.

For example, the organization/company had a Christmas party where a professional photographer photographed the event.

The organization/company requested the employee's consent to publish these images on the website, as well as on social networks and the channel YouTube. The organization/company had to separate the processing of personal data specifically for the website, especially for each social network, and in particular for the channel YouTube.

Each individual has the right to decide whether his or her personal data will be part of one of these media. It may be perfectly fine for an employee to have his/her photo posted on the website of the organization/company, but the same person may not want his/her photo to be marked countless times by different people on social networks and that these photos be shared.

Also, a person must have all the necessary information, especially about the fact that consent can be withdrawn at any time in the same way as it was given.

**9. The organization/company processes personal data through cookies on the website. In order to make it easier for visitors to access the site, they use pre-ticked consent boxes, and users can uncheck the box. We are aware that due to the law we are obliged to collect consent for cookies. To make it easier for our visitors on the website, we decided to offer them boxes where they can opt out from consent if they don't want this kind of data processing.**

Correct answer: **False**  
Your answer: **False**



The fact that organizations/companies are required by law to collect a consent for the processing of data through cookies on the website does not mean that website visitors must consent for this kind of processing of personal data.

Namely, the processing of personal data by means of cookies is generally not necessary (except for necessary or technical cookies) so the person has the right to decide whether to give consent.

For this reason, the consent box must not be pre-ticked, i.e., it must be empty, and if the person wants to give his/her consent, he can do so by clicking on the box.



Home GDPR topics About us About ARC2 project Webinars Anamarja Bartolić

GDPR topics > Legal Basis for Data Processing > Apply

## Determine the legal basis for processing personal data

Overview **Questionnaire**

### Part I – Identifying legal basis for data processing

\*1. In our business we do process personal data because such processing is prescribed by law.

- Yes  
 No

\*2. In our business we often enter into a contract with individuals.

- Yes  
 No

\*3. In our business we rely on Terms of service or similar document for processing of personal data.

- Yes  
 No

\*4. In our business, we sometimes make pre-contracts or send an offer to conclude a contract.

- Yes  
 No

\*5. In our business we process personal data to save or protect someone's life or vital interest such as health.

- Yes  
 No

\*6. In our business we process personal data in order to perform official tasks.

- Yes  
 No

\*7. In our business we process personal data in public interest.

- Yes  
 No

\*8. In our business, sometimes individuals can decide for themselves whether or not to consent to the processing of their personal data.

- Yes  
 No

\*9. In our business it is possible to stop data processing at the request of an individual.

- Yes

### Part II – If the SMEs rely on consent or legitimate interest there are more questions on validity of these legal basis

#### a. Consent

\*1. In our business, we use consent as a legal basis for the processing of personal data. When we ask for consent, we ask individuals to freely choose their own actions and make a decisions regarding data processing.

- Yes  
 No

\*2. In our business, we asked for several consents at the same time. For example, publishing a photo of the worker on the internal intranet, on the website with a description of the work that the person performs, and on the social media. We have provided a special box for each of these actions.

- Yes  
 No

\*3. In our business, we offer online services directly to children. Since we know that the child's age limit for giving consent in this context is 16 years old, we only seek consent if we have checked their age by age verification measures (and parental consent measures for younger children).

- Yes  
 No

\*4. It is our business philosophy to ensure withdrawal of a consent.

- Yes  
 No

#### b. Legitimate interest

\*5. In our business we do rely on legitimate interests for processing personal data.

- Yes  
 No

\*6. When relying legitimate interest(s) as a legal basis for the processing of personal data, first we have identified legitimate interest.

- Yes  
 No

\*7. When conducting legitimate interests assessment, we take into consideration impact on the persons whose data will be processed.

- Yes  
 No

\*8. When taking into consideration impact on the persons, we are thinking about the nature of personal data.

- Yes  
 No

\*9. When taking into consideration impact on the persons, we are thinking about the way of data being processed.

- Yes  
 No

\*10. When taking into consideration impact on the persons, we are thinking about possible harmful consequences for individual.

- Yes  
 No

**Practical module1:**  
Consists of set of questions that will help SMEs to identify legal basis for processing of personal data

## Practical module2: After completing the template, Olivia generates the consent form automatically.

Overview **Questionnaire**

\* Enter name/surname.

John Doe

\* Is it necessary to enter an identification specification?

Yes  
 No

\* Enter identification specification.

123578

\* Is it necessary to enter the name of the parent/legal representative?

Yes  
 No

\* Enter contact info.

john.doe@gmail.com

\* Enter type/category of the data.

name, surname, photo

\* Enter the processing what will be carried out.

publishing of personal data

### Consent for personal data processing

(according to the Article 7 of the GDPR)

#### Special notes:

- The consent for the child is given/authorised by the parent/holder of parental responsibility, except in the case of offering information society services directly to a child older than 14 years (the controller must make reasonable effort to verify it).
- it is necessary to inform the individual especially about the processing of data for automated decision-making individual's and about the possible risks of data transfer and appropriate safeguards which were taken.
- If the consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Name/surname  
John Doe

Identification specification  
123678

Contact info  
john.doe@gmail.com

Type/category of the data  
name, surname, photo

Processing to be carried out  
publishing of personal data

I CONSENT TO THE PERSONAL DATA PROCESSING FOR THE FOLLOWING SELECTED AND SPECIFIC PURPOSES:

on website of the organisation

on social media of organisation

I confirm that I am aware I may refuse this consent or withdraw it at any time. Also, I am aware that the processing is legal until the moment of withdrawal.

NOTE: Consent applies only to the stated processing purposes and the stated categories of personal data. The processing of personal data may not be used for any other purposes. The processing of these categories of personal data will be carried out in accordance with the GDPR. If an individual wishes to withdraw consent, he/she may do so in writing to the address: dpo@organisation.com, by e-mail to the address: dpo@organisation.com, or in person to the address of the registered office: XY.

Place/Date

Signature

## Conducting Legitimate Interest Assessment to demonstrate legitimate interest as lawful basis for processing of personal data

### Example:

The data controller is involved in organizing seminars and workshops across diverse fields. To promote these events, the data controller intends to send newsletters to the official email addresses of data protection officers. To obtain these email addresses, the data controller plans to collect publicly available email addresses from the websites of organizations.

- ✓ **After responding to 46 questions, Olivia generates Legitimate Interest Assessment form**

GDPR topics > Legal Basis for Data Processing > Apply  
**Legitimate interest assessment**

Overview **Questionnaire** Report

**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 data controller is engaged in organizing seminars/workshops in various fields. In order to sell seminars/workshops, the data controller wants to establish a new marketing

\* Your legitimate interest is in accordance with the law?

In recital 47 of the GDPR, it is stipulated that "processing personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". Considering that:

\* What benefits do you expect from processing?

informing data protection officers about our seminars and workshops and

\* Is there any benefit from processing for a third party?

yes

\* Is there a wider public benefit for processing?

yes



Overview

Questionnaire

Report

## 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

• Is the processing proportionate to that purpose?

YES

• Can you achieve the same purpose without processing?

NO

• Can you achieve the same purpose by processing less data or processing data in another more obvious or less intrusive way?

NO

Previous

Next

Save for later

GDPR topics > Legal Basis for Data Processing > Apply

## Legitimate interest assessment

Overview

Questionnaire

Report

## STEP 3: Balancing test

Assessment of the impact on the interests and rights and freedoms of individuals and an assessment of whether your legitimate interests outweigh data subject rights and freedoms.

### A. Nature of personal data

• Is this special category data or data on criminal convictions and offences?

NO

• Would data subjects likely consider this data specifically "private"?

NO

• Do you process data about children or data relating to other vulnerable groups?

NO

• Is the data of the data subjects related to their personal or professional capacity?

Professional capacity.

• Is this a large-scale personal data processing?



purpose, including the marketing activities mentioned above. In this regard, the data controller considers that the legitimate interest of the data controller outweighs the interest in protecting the personal data of the data protection officer who will be contacted.

**How have you assessed their legitimate expectations (e.g. through focus groups, market research, other types of consultation)?**

No.

**Are you transparent with the data subjects?**

Yes.

**If applicable, are you transparent with data subjects about the reuse of data for other purposes?**

Yes.

**Are there any other factors in certain circumstances that mean that individuals would or would not expect processing?**

No.

**C. Likely effect on individuals**

**What are the possible effects of processing on individuals?**

No possible negative effects.

**Will individuals lose control over the use of their personal data?**

No.

**What is the likelihood and severity of any potential negative impact on data subjects?**

Low.

**Are individuals likely to object to the processing or will they consider it intrusive?**

No.

**Will you explain the processing of personal data to individuals if they request it?**

Yes.

**Are there any legal consequences for respondents arising from the personal data processing (e.g. automated decisions)?**

No.

**Are you going to adopt some safeguards to minimize the likelihood of such negative impacts?**

The data controller has established protective measures to limit the undue impact of data processing on the data protection rights of the data protection officer. Primarily, the ability to object to data processing for marketing purposes has been provided, and data protection officers have the option to unsubscribe from the newsletter database. If an officer chooses to unsubscribe from the database, their personal data is permanently deleted, and they will no longer receive newsletters. Furthermore, in line with the principle of data minimization, no additional information about the officer is stored except for the email address.

Since the conclusions reached in all three previous steps are affirmative, we can rely on our legitimate interest for the processing of personal data in this case.

Comments:

We have demonstrated our legitimate interest.

Have you informed the respondents about their right to object to the processing of personal data?

**Will you offer individuals the opportunity to object?**  
Yes

The assessment was carried out by:

John Doe

Date:

10.06.2024.

**NEXT STEPS:**

- Document this assessment and review it as needed.
- If necessary, carry out a data protection impact assessment.
- Include details of your purposes and legal basis for processing in your policy/data protection notice/privacy policy.

## SMEs can complete the form (35 questions) and Olivia will generate the DPIA template

GDPR topics > Data protection impact assessment > Apply  
**Conduct a data protection impact assessment**

Overview **Questionnaire**

### STEP 1: Identification of need

\* Why do you think it is necessary to carry out a data protection impact assessment procedure?

The data controller, Package Ltd. (hereinafter referred to as the Company), is a provider of postal services (delivery service).

The Company is implementing a system to track the movements and locations of delivery and personal vehicles in its official fleet. Since the company's vehicles are operated by employees during and outside working hours, and these vehicles are also used for personal purposes, the Company is conducting data protection impact assessment based on the decision of the Data Protection Agency on the establishment and public disclosure of a list of types of processing activities subject to a data protection impact assessment requirement.

Previous Next

Save for later

GDPR topics > Data protection impact assessment > Apply  
**Conduct a data protection impact assessment**

Overview **Questionnaire**

This questionnaire contains 35 questions. Some questions will only appear if you answered one of the previous questions in a specific way.

The questionnaire can be filled as many times as wanted or needed.

Click on the fill questionnaire button to start filling it.

Fill questionnaire Edit questionnaire

Questionnaire was last submitted 11.06.2024 05:51

**Example: The Company is implementing a GPS system to track the movements and locations of delivery and personal vehicles in its official fleet. Since the company's vehicles are operated by employees during and outside working hours, and these vehicles are also used for personal purposes, the Company is conducting data protection impact assessment based on the decision of the Data Protection Agency on a list of types of processing activities subject to a data protection impact assessment requirement (this is processing that is likely to result in a high risk to the rights and freedoms of natural persons)**





Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The employees have been informed of processing of their personal data. Consultation has been conducted with the workers' council. We have consulted security experts and asked help from the data processor.

**STEP 4: ACCESS NECESSITY AND PROPORTIONALITY**

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The processing is based on the legitimate interests of the Company - processing personal data for the purpose of protecting the company's personnel and property and providing a better service. The Company has conducted an assessment of legitimate interest, and the assessment is documented.

The amount of data collected through the system has been minimized. The system records only vehicle data - type/use, license plate number..., and location data - movement, stops, idle time, speed, acceleration, sudden braking, exceeding the speed limit... that can be linked to the employee, or identify them.

We have signed the contract from Article 28 with the data processor. We don't transfer data to third countries. The purposes of processing can't be achieved in other way.

**STEP 5: IDENTIFY AND ASSESS RISKS**

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Unauthorized access to employees' personal data.	Possible	Serious	Medium
Data subjects, (employees) are unable to exercise their data protection rights.	Possible	Serious	High
Data loss	Low	Significant	Medium

**STEP 6: IDENTIFY MEASURES TO REDUCE RISKS**

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Unauthorized access to employees' personal data.	Implemented strict access controls to ensure that only authorized personnel have access to the GPS data. The strong authentication methods and role-based access controls are used to limit who can view or use the data. GPS data are encrypted both in transit and at rest to protect it from unauthorized access. It is ensured that encryption keys are securely managed.	Reduced	Low	Yes
Data subjects, (employees) are unable to exercise their data protection rights.	Provided clear and transparent information to employees about the purpose of GPS tracking, what data is being collected, how it will be used, and their rights regarding their data. Conducted training sessions to educate employees on data protection best practices.	Reduced	Low	Yes
Data loss	GPS data are stored in secure and compliant systems that adheres to industry standards for data security. Regularly review and update security measures to protect against data breaches.	Reduced	Low	Yes

**STEP 7: RECORD OUTCOME**

Item	Name / Date	Notes
Measures approved by:	Director of Company	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Director of Company	If accepting any residual high risk, consult the DPA before going ahead
DPO advice provided:	John Doe	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The risks have been reduced. The data processing can take place.		
DPO advice accepted or overruled by:	-	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	-	If your decision departs from individuals' views, you must explain your reasons
Comments		
This DPIA will be kept under review by:	John Doe	The DPO should also review ongoing compliance with DPIA

GDPR topics > Data Protection Officer (DPO) > Apply  
**Should I appoint a data protection officer?**

Overview Questionnaire

The user answers 3-10 questions and gets results on whether it is necessary to designate a data protection officer. If organisations/companies need to designate a data protection officer, they will be provided with further guidance on the appointment, position, and tasks of the data protection officer.

Also, in the case of an obligation to designate, a report to be provided to the data protection authority shall be generated.

Assessment of the need to designate a data protection officer

Note! Here are just some examples of when an organisation/company is obliged to designate a data protection officer.

A data protection officer should be designated (regardless of the number of employees!) in three specific cases:

- A) the processing is carried out by a public authority or body;
- B) where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects to a large extent; or
- C) where the core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

More on the EDPB Guidelines! <https://ec.europa.eu/newsroom/article29/items/612048>

Connected courses




**OLIVIA**  
GDPR topics

Data Protection Officer (DPO)



- \* 2. One of the tools that my organisation/company uses in its business is a loyalty program.
  - Yes
  - No
- \* 3. You are engaged in providing tourist/sports/wellness/fitness/health services. In your business, you offer wearable electronic devices that track individuals' habits or otherwise collect their health data, and based on the results collected, your organisation/company makes health recommendations.
  - Yes
  - No
- \* 4. You use GPS to track vehicles in your organisation/company to ensure that your drivers do their job efficiently and safely.
  - Yes
  - No
- \* 5. Your organisation/company has the right to contract the acceptance and issuance of bank cards, as well as to manage business operations in the countries for which it has sub-franchise rights or your organization/company is selling insurance.
  - Yes
  - No
- \* 6. In your business you conduct scientific research (e.g., health clinic).
  - Yes
  - No
- \* 7. Your organisation/company provides services of analysis of traffic on websites for the purpose of targeted advertising and marketing for organisations/companies whose main activity is the distribution of goods or services.
  - Yes
  - No
- \* 8. Your organisation/company is engaged in the provision of occupational health services to multiple companies as an external processor.
  - Yes
  - No

<https://olivia-gdpr-arc.eu/hr>

<https://olivia-gdpr-arc.eu/italian/it>

