

# Consent to the Processing of Personal Data

---

(GDPR – Purpose: sending job offers and processing data)

## 1. Who is the controller of personal data?

---

The controller of your personal data is:

**Dilibees s.r.o.** Korunní 2569/108,

ID: 11848987

VAT ID: CZ11848987

Email: info@dilibees.com

Phone: +420702070250

The user can contact us regarding any questions about personal data through:

- **Email:**
- **Phone:**
- **Postal address**

The controller is responsible for ensuring that your personal data is processed securely, transparently, and in accordance with applicable legal regulations.

If the controller appoints a Data Protection Officer (DPO), their contact details will be added here.

## Privacy Statement

This document describes:

- what personal data we collect,
- for what purpose we process it,
- to whom we may transfer it,
- what rights you have as a user,
- and how we protect your data.

The purpose of this document is to provide users with clear and transparent information about how we handle personal data in the context of job mediation.

## **Who is this document for?**

This document is intended for all natural persons who:

- create an account on our platform,
- are seeking a job opportunity,
- use our job mediation services,
- or provide us with personal data for the purpose of receiving a job offer.

The document does not apply to the controller's employees or persons acting on behalf of companies looking for workers (other provisions apply to them).

## **2. What personal data do we process?**

---

We only process data that is necessary for providing our services, especially for mediating job offers, managing user accounts, providing other services, etc.

We divide personal data into the following categories:

### **2.1 Identification data**

This data serves for your unique identification:

- first name
- last name
- date of birth (if voluntarily provided by the user)
- gender (optional)

### **2.2 Contact data**

Data needed for communication and sending job offers:

- email address
- phone number

- home address
- country or region where you are looking for work

## **2.3 Work and professional information**

Data related to your work profile and qualifications:

- current profession (e.g., welder, electrician, CNC operator...)
- specialization (e.g., MIG/MAG/TIG welding method)
- length of practice
- previous work experience
- preferred job position
- preferred work location
- availability (immediately / from a certain date)

## **2.4 Qualification and skills data**

Data necessary for assessing suitability for specific job offers:

- professional certificates (e.g., welding certificates EN ISO 9606)
- training, courses, exams
- language skills
- professional skills (e.g., reading technical drawings, working with CNC machines)

## **2.5 Documents and files uploaded by the user**

(Used exclusively for the purpose of employment mediation.)

- curriculum vitae (CV)
- cover letters
- certificates, attestations, licenses
- photos or documents that the user voluntarily uploads

The controller never requires any sensitive data, such as data on health status, racial origin, political opinions, or sexual orientation.

## **2.6 Technical and analytical data**

Data necessary for the operation of the platform:

- IP address
- device information
- login logs
- cookies (technical, security, analytical)
- information about activity in the account (profile completion, responses to offers)

This data is used for security, account functionality, and service improvement.

## **2.7 Voluntarily provided data**

The user can at any time add other information that may help in selecting a suitable job offer, for example:

- availability for overtime
- preferred type of contract
- expected salary
- equipment owned (e.g., own welding machine, tools)

## **2.8 Communication data**

Data obtained during communication between us and the user:

- email communication
- telephone communication
- messages sent via the platform

This information is used only to handle requests and improve services.

## **3. Purposes of personal data processing**

---

We process personal data only to the extent necessary for the provision of our services. As a job intermediary, we process data for the purposes listed below:

### **3.1 Creating and managing a user account**

We need personal data for:

- user registration,
- enabling login to the system,
- maintaining and updating the user profile,
- managing account security.

This purpose is necessary for using our platform.

### **3.2 Providing job mediation services**

We process data to help the user get a job offer that matches their profile. This includes, in particular:

- evaluating suitability for specific job positions,
- creating and presenting the user's profile to potential employers,
- recommending positions according to qualifications,
- communication between the applicant and our team regarding job opportunities.

### **3.3 Transfer of profile and personal data to potential employers**

In order to find a suitable job position, we may transfer your profile to:

- employers,
- personnel agencies,
- recruitment departments of companies,
- partners looking for workers.

The purpose of the transfer is exclusively to obtain a job offer corresponding to your skills and experience.

The transfer only occurs after you have given your explicit consent.

We never transfer data to third parties for their own marketing.

### **3.4 Sending job offers and commercial communications**

Processing includes:

- sending job offers by email, phone, in our software, WhatsApp, or via SMS,
- notifications of new positions according to the profile,
- information about the progress of the recruitment process.

This purpose is based on the user's separate consent (direct marketing).

### **3.5 Communication with the user**

We use the data to:

- answer queries,
- confirm registration,
- resolve technical problems,
- provide support in selecting a job offer.

This includes communication by phone, email, and via the platform.

### **3.6 Improving the quality of services and the functioning of the platform**

For the purpose of security and system optimization, we process:

- login logs,
- technical data,
- user behavior on the platform (e.g., responses to offers).

This data is used to improve the platform's functions, security, and personalization of services.

### **3.7 Fulfilling legal obligations**

In some cases, we may process data because we are required to do so by law, for example:

- the obligation to submit documents to control authorities,
- the obligation to retain certain data for a specified period (if arising from the law).

This applies in particular to cases where the company would also function as a temporary employment agency.

### **3.8 Protection of rights and legitimate interests**

We may also use the data to:

- resolve disputes,
- prevent fraud,
- protect our systems and users,
- enforce contractual obligations.

This purpose is based on the legitimate interest of the controller.

## **4. Legal bases for personal data processing**

---

We process personal data only when one of the legal bases listed in Art. 6 of the GDPR exists for their processing. Below we list the individual purposes and their corresponding legal bases.

### **4.1 User consent (Art. 6(1)(a) GDPR)**

This is the most important legal basis for job mediation. Based on your consent, we process in particular:

#### **a) Transfer of your profile to third parties**

- employers,
- personnel agencies,
- partners who are looking for workers.

This consent is necessary because without it, your profile cannot be forwarded for consideration for a specific job position.

#### **b) Sending job offers (direct marketing)**

This category includes:

- sending job offers by email,
- sending offers by phone or SMS,
- notifications of new positions.

#### **c) Voluntarily provided additional data**

E.g., photo, CV, preferred salary, specific skills.

The user can withdraw consent at any time without affecting the use of the basic functions of the account.

### **4.2 Performance of a contract (Art. 6(1)(b) GDPR)**

This legal basis applies when:

- the user creates and uses an account,
- uses the job search service,
- we manage their profile,
- we provide the platform's functionalities.

Data processing is necessary for us to provide the user with the service they have actively chosen.

### **4.3 Legitimate interest of the controller (Art. 6(1)(f) GDPR)**

We use this legal basis in cases where:

a) **we improve the security of the platform** – fraud detection, system protection, prevention of misuse.

b) **we analyze technical data** – login logs, cookies for security and functionality, error diagnostics.

c) **we record basic statistics** – for example, number of registrations, account activity, non-personal analytics.

We never use legitimate interest for transferring data to third parties or for marketing.

#### **4.4 Performance of a legal obligation (Art. 6(1)© GDPR)**

In some cases, we are obliged to process data because it is required by law — typically, for example:

- retention of records for inspection purposes (in the case of temporary agency employment),
- fulfillment of obligations towards state authorities.

This legal basis will only apply in situations where job mediation requires the fulfillment of specific legal obligations (e.g., work within the framework of temporary agency employment).

#### **4.5 Protection of vital interests (Art. 6(1)(d) GDPR)**

In exceptional situations, we may process data for the purpose of:

- protecting the life or health of the user,
- providing data in urgent situations (e.g., contacts in case of danger).

In practice, this legal basis is used only rarely.

## **5. Sharing personal data with third parties**

---

For the purpose of employment mediation, personal data may be transferred to third parties. The transfer occurs exclusively on the basis of your consent, which can be withdrawn at any time. Below we explain to whom, when, and why your data may be transferred.

## 5.1 To whom may data be transferred

Your personal data may be transferred to the following categories of recipients:

- a) **Potential employers** Companies that are currently looking for employees in your profession and have open job positions.
- b) **Personnel agencies and recruitment partners** Intermediaries who search for workers in technical professions for their clients (e.g., welders, electricians, locksmiths, CNC operators).
- c) **HR service providers** Entities carrying out pre-selection, verification of qualifications, or administrative processing of data within the recruitment process.
- d) **Providers of IT, hosting, and software solutions** These recipients only have access to the technical data necessary for the operation of the platform and not to the content of your profile, unless this is part of the contractual service.

## 5.2 For what purpose is data transferred

The purpose of the transfer is exclusively the mediation of a job opportunity, specifically:

- offering a suitable job position to the user,
- contacting the user by the employer or agency,
- assessment of qualifications for the given position,
- arranging an interview or test,
- completion of the recruitment process.

Data is never transferred for the marketing purposes of third parties.

## 5.3 What data may be transferred

Only data relevant to the job position may be transferred, in particular:

- first and last name,
- email / phone,
- profession and qualifications,

- certificates and skills,
- work experience,
- information provided in the curriculum vitae and work profile,
- availability and preferred location.

Sensitive data (e.g., health status, religious beliefs) is never transferred.

## **5.4 Conditions for data transfer**

A transfer only takes place if:

- the user has given explicit consent,
- there is an open job position corresponding to the profile,
- the recipient undertakes to protect personal data in accordance with the GDPR,
- security is ensured during data transmission.

Each transfer is minimized to only the necessary scope of data.

## **5.5 Transfer of data outside the European Union**

If the recipient is outside the EU or EEA, the transfer only takes place if:

- the country has a recognized adequate level of protection (e.g., Switzerland),
- or Standard Contractual Clauses (SCC) are concluded,
- or there is another guaranteed legal basis under the GDPR.

The user will always be informed in such a case.

## **5.6 Responsibility of recipients**

All third parties to whom your profile may be transferred:

- have a data protection agreement with us,
- are bound by confidentiality,
- may not use the data for any purpose other than the job offer,
- are obliged to delete the data after the selection process is completed.

## 5.7 Your rights regarding data transfer

The user has the right to:

- be informed of all recipients,
- withdraw consent to the transfer of data,
- request restriction of transfer,
- request deletion of data from recipients,
- withdraw their profile from recruitment.

The controller will ensure that requests are forwarded to the recipients so that they can also fulfill them.

## 6. Personal data retention period

---

We retain personal data only for the time necessary, which corresponds to the purposes for which the data was obtained. The retention period is set to take into account the needs of job applicants, the requirements of employers, and legal obligations.

### 6.1 Retention of data for the purpose of job mediation

We retain the data necessary for searching for job offers and transferring the profile to employers:

– for a period of **3 years from registration or the user's last activity**, unless the user withdraws their consent earlier.

Activity means, for example:

- updating the profile,
- responding to a job offer,
- logging into the account.

If there is no activity for 3 years, the profile will be automatically anonymized.

## 6.2 Retention of data based on consent

If processing is based on consent (e.g., forwarding the profile to an employer, sending job offers):

- we retain the data for the duration of the consent,
- after its withdrawal, we delete or anonymize the data without undue delay.

## 6.3 Retention of data for the fulfillment of legal obligations

In the event that a legal obligation arises to retain certain data (typically in the case of temporary agency employment, international work permits, etc.):

- we retain the data for the period stipulated by law.

This can be, for example, 3–10 years depending on the type of documentation.

If the controller does not have such an obligation, this part does not apply.

## 6.4 Technical data

We retain technical data from logs and system records:

- for **12 months**, and then they are automatically deleted or archived in an anonymous form.

This includes:

- IP addresses,
- login records,
- records of errors and security incidents.

## 6.5 Anonymization of personal data

After the specified retention period has expired, the data will be:

- securely deleted, or
- irreversibly anonymized (the user can no longer be identified).

Anonymized data may only be used for statistical purposes and for improving services.

## 6.6 User's right to request earlier deletion

The user has the right to request at any time:

- immediate deletion,
- restriction of processing,
- removal of their profile,
- cancellation of the account.

The controller will perform the deletion without undue delay (usually within 30 days), unless there are other legal retention obligations.

## 7. How we protect data

---

We protect your personal data using a combination of technical, organizational, and security measures that comply with GDPR requirements and current data protection standards. The security and trust of our users are our priority.

### 7.1 Technical security measures

To protect personal data, we use in particular:

#### a) Data encryption

- encryption of data transmission using HTTPS / SSL,
- encryption of sensitive data in databases.

#### b) Secure servers and infrastructure

- servers with a high degree of security,
- regular updates and security patches,
- access restricted to authorized personnel.

#### c) Strong authentication mechanisms

- minimum security requirements for passwords,
- password hashing (we never store passwords in a readable form),
- protection against brute-force attacks.

#### d) **Protection against cyber attacks**

- firewall,
- anti-malware systems,
- monitoring of suspicious activities,
- attack detection and prevention (IDS/IPS).

### **7.2 Organizational security measures**

To ensure the correct handling of personal data, we also implement internal processes:

a) **Access only for authorized persons** Access to data is only granted to persons who need it for their work (the need-to-know principle).

b) **Training and confidentiality obligations** All employees who come into contact with data:

- are regularly trained in the area of GDPR,
- are bound by confidentiality,
- sign internal confidentiality agreements.

#### c) **Internal rules for data handling**

- access is audited,
- data is not processed outside of designated applications,
- we use secure tools for sharing data with partners.

### **7.3 Measures towards third parties**

If personal data is transferred to third parties (e.g., employers, personnel agencies, IT providers):

a) they must delete the data after the selection process is completed.

### **7.4 Regular checks and testing**

To ensure long-term security, we perform:

- regular security checks,
- continuous software updates,
- backup tests,
- security audits,
- monitoring of access and data changes.

## 7.5 Security incidents

In the event of a security breach (data leak, unauthorized access):

- we always proceed according to the GDPR,
- we assess the incident within 72 hours,
- we inform the Office for Personal Data Protection (if it is mandatory),
- we inform the affected users (if there is a probable risk of harm).

Our goal is to minimize the impact and ensure a quick remedy.

## 8. User rights

---

As a user of our platform, you have full control over your personal data. The GDPR provides you with a number of rights that we respect and allow you to easily exercise. Below is an overview of the individual rights and their explanation.

### 8.1 Right of access to personal data (Art. 15 GDPR)

You have the right to know:

- what data we process about you,
- from what sources it comes,
- why we process it,
- to whom it has been or will be transferred,
- how long we store it.

Upon request, we will provide you with a copy of all processed data.

## **8.2 Right to rectification of personal data (Art. 16 GDPR)**

If you find that your data is:

- inaccurate,
- out of date,
- incomplete,

you can request its correction or completion. We will carry out the correction without undue delay.

## **8.3 Right to erasure – “right to be forgotten” (Art. 17 GDPR)**

You can request the erasure of personal data if, for example:

- we no longer need the data for the provision of services,
- you withdraw your consent,
- the processing was unlawful,
- you want to cancel your account,
- you no longer want to be in our database of applicants.

We will carry out the erasure without undue delay, unless another law imposes an obligation on us to retain the data.

## **8.4 Right to restriction of processing (Art. 18 GDPR)**

You can exercise this right if:

- you wish to temporarily suspend the processing of data,
- you suspect that the data is incorrect,
- you do not want the data to be transferred to third parties,
- your request or objection is being resolved.

We will only store your data, but not process it.

## **8.5 Right to object to processing (Art. 21 GDPR)**

You can object in particular to:

- profiling,
- sending job offers (direct marketing).

If you object to marketing, we will immediately stop sending marketing communications.

## **8.6 Right to data portability (Art. 20 GDPR)**

You can request from us:

- an overview of your personal data in a structured,
- commonly used and machine-readable format,

or you can request its transfer to another job intermediary.

## **8.7 Right to withdraw consent to the processing of data**

Consent given for the purposes of:

- sending job offers,
- transferring the profile to employers,
- processing of voluntary data,

you can withdraw at any time.

Upon withdrawal of consent, we will immediately terminate the processing of data that was based on this consent.

## **8.8 Right to lodge a complaint with a supervisory authority**

If you believe that we are not handling your personal data correctly, you have the right to lodge a complaint with:

**The Office for Personal Data Protection (ÚOOÚ)** Pplk. Sochora 27 170 00 Prague 7  
Czech Republic Web: [www.uoou.cz](http://www.uoou.cz)

## 8.9 How to exercise your rights

You can exercise your rights:

- by e-mail to: info@dilibees.com
- via the form in your user account,
- or in writing to the controller's address.

We process requests without undue delay, no later than within **30 days**.

## 9. Automated decision-making and profiling

---

Within our platform, we use certain elements of automated processing that help recommend suitable job offers. However, this processing is not fully automated decision-making that would have legal or similarly significant effects on the user under Art. 22 of the GDPR. Below, we explain what type of profiling we perform, why, and how the user is protected.

### 9.1 What is profiling?

Profiling is the automated processing of personal data that evaluates certain aspects of the user — for example, their:

- profession,
- qualifications,
- certificates,
- experience,
- preferred location,
- skills,
- availability.

Based on this data, our system recommends job offers that match the user's profile.

### 9.2 How profiling works

The system can:

- compare the user's qualifications and skills with the requirements of job positions,
- sort offers by relevance,
- notify of available positions corresponding to the profile,
- evaluate through an algorithm how much the user meets the criteria of the position (e.g., percentage match).

This is a support for the selection of job offers — the final decision is always up to the user or the employer.

### **9.3 What is not automated decision-making**

Based on profiling:

- we do not decide on acceptance or rejection for a job,
- we do not make legal decisions,
- no obligations arise for the user,
- no negative legal consequences arise.

The system recommends, but does not decide.

The decision on whether the user will be contacted is always made by a real person — an employer, an agency, or a recruitment specialist.

### **9.4 Why we use profiling**

We use profiling to:

- increase the user's chances of finding a suitable job,
- offer only relevant job offers,
- not overwhelm the user with unsuitable positions,
- speed up the job search process.

The goal is to provide quality services, not to limit the user.

## 9.5 User rights in relation to profiling

You have the right to:

- request an explanation of the profiling method,
- object to profiling,
- request that some data not be included in the algorithm,
- request human intervention if the result of the profiling were to have a major impact (which does not normally happen in our service).

If you refuse profiling, the system will stop recommending offers, and this may affect the quality of the services provided.

## 9.6 Protective measures

To ensure fair treatment:

- profiling is limited to only necessary data,
- the algorithms are regularly checked,
- we minimize the risk of errors and incorrect conclusions,
- we do not use sensitive data (e.g., health status, race, religion),
- profiling is not used to exclude users.

# 10. Cookies and similar technologies

---

Our platform uses cookies and other technologies to ensure proper functioning, security, and to improve the user experience. This section explains what types of cookies we use, why we use them, and how you can control their use.

## 10.1 What are cookies?

Cookies are small text files that are stored on your device (phone, computer, tablet) when you visit our website or use our application. They do not contain any malicious code or personal data that would in itself allow for your identification.

## 10.2 Types of cookies we use

### a) **Essential (technical) cookies**

These cookies are necessary for the basic functioning of the platform. Without them, it would not be possible to:

- log in to your account,
- keep you logged in,
- display the pages correctly,
- ensure security and data protection,
- work with forms and submit data.

These cookies cannot be disabled.

### b) **Functional cookies**

They improve user comfort and allow for:

- remembering your preferences,
- personalization of display,
- better functioning of user elements.

### c) **Analytical and statistical cookies**

They help us understand how users use the service. For example, they measure:

- the number of visits,
- behavior on the site (clicks, time spent),
- technical errors,

and allow us to improve the platform. We use, for example:

- Google Analytics (in anonymized mode),
- internal statistical tools.

### d) **Marketing cookies**

We only use these if you give your consent. These cookies can:

- personalize the display of job offers,
- measure the effectiveness of campaigns,
- help to better target job offers.

We do not transfer data to third parties for commercial marketing – only for job offers, if you agree to it.

### **10.3 Why we use cookies**

We use cookies mainly to:

- ensure the functionality and security of the platform,
- maintain login and user settings,
- optimize system performance,
- analyze user behavior,
- improve the quality of our services,
- recommend relevant job offers.

### **10.4 Managing and disabling cookies**

In your browser settings, you can:

- disable cookies,
- delete them,
- allow only some,
- set a notification when they are stored.

If you disable essential cookies, the platform may not function correctly.

Within the platform, you can:

- reject analytical or marketing cookies in the cookie bar,
- change your preferences at any time later.

### **10.5 Third-party cookies**

Some tools may store their own cookies:

- Google Analytics (anonymized analytics),
- security and hosting providers,
- providers of advertising services (only with your consent).

These entities are contractually bound to comply with the GDPR.

## 10.6 Cookie retention period

Each type of cookie has a different retention period:

- essential cookies: for the duration of the session,
- functional cookies: usually 1–12 months,
- analytical cookies: 3–24 months,
- marketing cookies: 3–12 months (only with consent).

After the expiration date, the cookies are automatically deleted.

## 10.7 Other tracking technologies

In addition to cookies, we may also use:

- local storage,
- web beacons,
- tracking pixels.

They are used only for technical and analytical purposes, or for recommending job positions.

# 11. Transfer of personal data outside the European Union

---

In specific cases, your personal data may be transferred to recipients located outside the European Union (EU) or the European Economic Area (EEA). A transfer only occurs when it is necessary for the provision of our services and an adequate level of protection under the GDPR is always ensured.

## 11.1 When a transfer may occur

A transfer of data outside the EU/EEA may occur in these situations:

- we use cloud services or IT providers with servers outside the EU (e.g., USA),
- we transfer data to employers who are based outside the EU,
- we use analytical or statistical tools operated outside the EU,
- we provide services to users or companies in countries outside the EU.

## 11.2 Transfer to countries with an adequacy decision

If the recipient of the data is in a country that the European Commission has designated as safe (has a so-called “adequate level of protection”), the data can be transferred without further authorization.

These countries include, for example:

- Switzerland,
- Norway,
- Iceland,
- Liechtenstein,
- Japan,
- Canada (parts),
- South Korea.

## 11.3 Transfer to countries without an adequacy decision

If the recipient is located in a country that does not have a recognized adequate level of protection (e.g., the USA after the invalidation of the Privacy Shield), it is necessary to implement other protective measures, for example:

a) **Standard Contractual Clauses (SCC)** These are contractual documents approved by the European Commission, which the data recipient must comply with.

b) **Additional technical measures**

- encryption,

- pseudonymization,
- restriction of access.

### c) **Contractual obligations of the recipient**

- use of data only for the purpose of job mediation,
- obligation to delete data after the process is completed,
- prohibition of further transfer.

Without meeting these conditions, a transfer does not occur.

## **11.4 User information**

If your profile is transferred to a subject outside the EU/EEA:

- we will always inform you about it,
- we will state the specific country and category of the recipient,
- we will explain the legal protection that is used.

We will not transfer your profile without your consent.

## **11.5 Transfer of data outside the EU for the purpose of job offers**

If the job offer is from an employer from a country outside the EU, it may be necessary to transfer your profile directly to this subject.

However, this only happens:

- on the basis of your explicit consent,
- if the offer is relevant to your profile,
- if the security measures mentioned above are met.

## **11.6 Guarantees of your data protection**

To ensure security in international data transfers:

- we verify the trustworthiness of recipients,
- we conclude contracts on the processing of personal data,

- we check compliance with GDPR principles,
- we use the minimum necessary scope of transferred data.

## 12. Final provisions

---

### 12.1 Effectiveness of the document

This document “Principles of Personal Data Processing (GDPR)” becomes effective on:

**[effective date]**

and is continuously updated according to changes in legislation, technology, and internal processes.

### 12.2 Changes to these principles

We reserve the right to update these principles at any time, especially if:

- there is a change in legal regulations,
- the method of providing services changes,
- new technologies begin to be used,
- the purposes of personal data processing are expanded or changed.

In case of significant changes:

- we will notify users of the change in an appropriate manner (e-mail, notification in the profile, pop-up),
- re-granting of consent may be required if the changes concern the purposes or scope of processing.

### 12.3 Availability of the document

The current version of these principles is always available:

- on our website,
- in the user account on the platform,
- by e-mail upon request.

## 12.4 Contacts for questions regarding personal data protection

If you have questions, comments, or want to exercise your rights, contact us:

**Email:** [company contact] **Phone:** [company contact] **Postal address:** [registered office address]

If we have a Data Protection Officer (DPO), you can contact them at: **[DPO contact – if one exists]**

## 12.5 Interpretation of the document

This document is intended for users of our platform and is interpreted in accordance with:

- Regulation (EU) <sup>2016</sup>/<sub>679</sub> (GDPR),
- Act No. <sup>110</sup>/<sub>2019</sub> Coll., on the processing of personal data,
- the Act on Certain Information Society Services,
- related legal regulations of the Czech Republic or the state where the controller operates.

## 12.6 Consent to the document

By using our platform or by giving consent in the registration form, you confirm that:

- you have read these principles,
- you understand their content,
- you agree to their terms.

Without granting certain consents (e.g., transfer of the profile to an employer or sending job offers), it is not possible to fully use all the functions of the platform.

## 12.7 Archiving and demonstrability

For the purpose of fulfilling GDPR requirements, we retain:

- records of consents granted,
- records of consent withdrawals,

- technical records of document updates.

Thanks to this, we can prove that the processing was carried out in accordance with the legislation.