



## Principles of Processing Personal Data

Valid as of July 1, 2023

**Principles of Processing Personal Data** (hereinafter – the Principles) describe how SIA Trinat processes Personal Data. To contact Trinat and/or exercise the rights of a data subject, see Sections 11 and 12 of the Principles.

Thank you for choosing to be part of our community at SIA Trinat (“Company”, “we”, “us”, or “our”). We are committed to protecting your personal information and your right to privacy. When you visit our website <https://trinat.lv> and use our services, you trust us with your personal information. We take your privacy very seriously and seek to explain to you in the most transparent way possible what information we collect, how we use it, and what rights you have concerning it. We hope you take the time to read it carefully, as it is crucial.

If there are any terms in these Principles that you disagree with, please discontinue using our Sites and our services. These Principles apply to all information collected through our website (such as <https://trinat.lv>) and/or any related services, sales, marketing, or events (we refer to them collectively as the “Services”).

Please read carefully; it will help you make informed decisions about sharing your personal information with us.

## 1. Definitions

- **Personal Data** means any information directly or indirectly related to the Client.
- **Processing** means any operation or set of operations performed regarding the Personal Data, whether performed by automated means, such as collection, recording, organisation, storage, adaptation, alteration, retrieval, use, combination, erasure, or destruction.
- **Client** means any natural person or a legal entity who uses, has used, or has expressed a wish to use the Services or is in other way related to the use and/or user of any of the Services and/or has any other relationship with SIA Trinat established before these Principles entered into force.
- **Data Controller** means anyone who, alone or jointly with others, determines the purposes and means of Processing Personal Data. For the Processing of Personal Data described in these Principles, SIA Trinat is the Data Controller.
- **Data Processor** means anyone who Processes Personal Data on behalf of the Data Controller.
- **Recipient** means a natural or legal person, public authority, or another body to whom SIA Trinat is entitled to disclose Personal Data.
- **Data Protection Legislation** means the applicable EU and national data protection legislation that SIA Trinat is subject to, for example, Regulation (EU) 2016/679 (General Data Protection Regulation or the GDPR).
- **Regulatory Legislation** means the applicable legal acts that SIA Trinat is subject to, for example, relating to anti-money laundering, banking secrecy, commercial activity, data protection, taxes, bookkeeping, credit, consumer credit, payment, payment services, insurance, leasing, investment, and financial business.
- **SIA Trinat** means us as a legal entity with a registered office in Latvia.

## 2. Personal Data processing

**In Short:** We collect the personal information you provide us, such as name, address, contact information, passwords and security data, payment information, and social media login data.

We collect personal information that you voluntarily provide to us when registering at the Services, expressing an interest in obtaining information about us or our products and services, when participating in activities on the Services (such as posting messages in our online forums or entering competitions, contests or giveaways, the Network) or otherwise contacting us.

The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make and the products and features you use. The personal information we collect can include the following:

### **2.1 Publicly Available Personal Information**

We collect first name, maiden name, last name, nickname, phone numbers, email addresses, business email, business phone number, and other similar data.

### **2.2 Personal Information Provided by You**

We collect CV and other job application data such as background checks, financial information (credit card number, purchase history, invoices), and other similar data.

### **2.3 Credentials**

We collect passwords, password hints, and similar security information used for authentication and account access.

### **2.4 Social Media Login Data**

We allow you to register or sign in using social media account details, like your Facebook, Twitter, or other social media account. If you choose to register this way, we will collect the Information.

All personal information you provide must be true, complete and accurate, and you must notify us of any changes to such personal information.

## 2.5 Session Video Recordings

While you visit our App or the Website, we reserve the right to capture your session, which might contain various forms of data. We use these recordings to help debug problems and understand user behaviour using our App and Website to improve your User Experience and track critical issues.

We do not directly reference our customers using user identifiers or device information in Session Video Recordings.

Please be aware that we seriously respect your privacy and understand how important it is to keep your sensitive information away, so under any circumstances, we do not record:

- Banking and Payment information with some examples include:
  - credit cards;
  - legal address;
  - bank account number;
- Sensitive information with some examples to include:
  - phone numbers;
  - personal address;
- Other sensitive information which can directly link to your identity

Meanwhile, we leave you the right to remove all Session Video Recordings. Please see Section XI to learn how to file our DPO with such a request.

### Automatically Collected Information

**In Short:** Some information – such as IP address and/or browser and device characteristics – is collected automatically when you visit our Services.

We automatically collect certain information when you visit, use or navigate the Services. This information does not reveal your specific identity (like your name or contact information). Still, it may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services and other technical details. This information is primarily needed to maintain the security and operation of our Services and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies.

### **Online Identifiers**

We collect devices, tools, and protocols, such as IP (Internet Protocol) addresses, cookie identifiers, or others, such as those used for analytics, marketing, and other similar data.

### **How do we use your information?**

**In Short:** We process your information based on legitimate business interests, the fulfilment of our contract with you, compliance with our legal obligations, and/or your consent.

We use personal information collected via our Services for various business purposes described below. We process your personal data for these purposes in reliance on our legitimate business interests to enter into or perform a contract with you, with your consent, and/or for compliance with our legal obligations. We indicate the specific processing grounds we rely on next to each purpose listed below.

### **To facilitate account creation and logon process**

Suppose you choose to link your account with us to a third-party account (such as your Google or Facebook account). In that case, we use the information you allowed us to collect from those third parties to facilitate the account creation and logon process for the performance of the contract.

### **Fulfil and manage your orders**

We may use your information to fulfil and manage your orders, payments, returns, and exchanges through the Services.

### **Deliver targeted advertising to you**

We may use your information to develop and display content and advertising (and work with third parties who do so) tailored to your interests and/or location and to measure its effectiveness.

#### **Request Feedback**

We may use your information to request feedback and contact you about using our Services.

#### **To protect our Services**

We may use your information to keep our Services safe and secure (for example, for fraud monitoring and prevention).

#### **To enable Client-to-client communications**

We may use your information to enable Client-to-client communications with each Client's consent.

#### **To enforce our terms, conditions and policies for Business Purposes, Legal Reasons and Contractual**

Respond to legal requests and prevent harm. If we receive a subpoena or other legal request, we may need to inspect the data we hold to determine how to respond. To deliver services to the Client. We may use your information to provide you with the requested service.

#### **Respond to Client inquiries/offer support to Clients.**

We may use your information to respond to your inquiries and solve any potential issues you might have with the use of our Services.

### **3. Information Exchange**

**In Short:** We only share information with your consent to comply with laws, to provide you with services, to protect your rights, or to fulfil business obligations.

**We may process or share data based on the following legal basis:**

- **Consent:** We may process your data if you have permission to use your personal information for a particular purpose.
- **Legitimate Interests:** We may process your data when reasonably necessary to achieve our legitimate business interests.
- **Performance of a Contract:** Where we have entered a contract with you, we may process your personal information to fulfil the terms of our agreement.
- **Legal Obligations:** We may disclose your information where we are legally required to do so to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal processes, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).
- **Vital Interests:** We may disclose your information where we believe it is necessary to investigate, prevent, or act regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

### **Business Transfers**

We do not share or transfer your information in connection with or during negotiations of any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

### **Other Clients**

When you share personal information or otherwise interact with public areas of the Services, such personal information may be viewed by all Clients and may be publicly distributed outside the Services in perpetuity. If you interact with other Clients of our Services and register through a social network (such as Facebook), your contacts on the social network will see your name, profile photo, and descriptions of your activity. Similarly, other Clients can view your activity reports, communicate with you within our Services, and view your profile.

## 4. Cookies and other tracking technologies

**In Short:** We may use cookies and other tracking technologies to collect and store your information.

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information.

## 5. Social logins

**In Short:** If you choose to register or log in to our services using a social media account, we may have access to certain information about you.

Our Services allow you to register and log in using your third-party social media account details (like your Facebook or Gmail logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The profile Information we receive may vary depending on the social media provider concerned but will often include your name, e-mail address, friends list, profile picture, and other information you choose to make public.

We will use the information we receive only for the purposes described in these Principles or otherwise made clear to you on the Services. Please note that we do not control, and are not responsible for, other uses of your personal information by your third-party social media provider. We recommend that you review their Privacy Policy to understand how they collect, use and share your personal information and how you can set your privacy preferences on their sites and apps.

## 6. Personal information lifetime

**In Short:** We keep your information for as long as necessary to fulfil the purposes outlined in these Principles unless otherwise required by law.

We will only keep your personal information for as long as necessary for the purposes set out in these Principles unless a more extended retention period is required or permitted by



law (such as tax, accounting, or other legal requirements). No purpose in these Principles will need us to keep your personal information for longer than 2 years past the termination of the Client's account.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymise it, or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

## 7. Protecting your personal information

**In Short:** We aim to protect your personal information through organisational and technical security measures.

We have implemented appropriate security measures designed to protect your personal information. However, the internet is 100% secure. Although we will do our best to protect your personal information, the transmission of personal information to and from our Services is at your own risk. You should only access the services within a secure environment.

## 8. Client's privacy rights

**In Short:** In some regions, such as the European Economic Area, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.

In some regions (like the European Economic Area), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; and (iv), if applicable, to data portability. In certain circumstances, you may also have the right to object to processing your personal

information. Please use the contact details in Section 11 to make such a request. We will consider and act upon any request following applicable data protection laws.

If we rely on your consent to process your personal information, you can withdraw your consent at any time. Please note, however, that this will not affect the lawfulness of the processing before its withdrawal.

Suppose you are a resident of the European Economic Area, and you believe we are unlawfully processing your personal information. In that case, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: [http://ec.europa.eu/justice/data-protection/bodies/authorities/index\\_en.htm](http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm).

### **Account Information**

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Contact us using the contact information from Section 11
- Log into your account settings and update your user account

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, some information may be retained in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our Terms of Use and/or comply with legal requirements.

### **Cookies and similar technologies**

Most Web browsers are set to accept cookies by default. You can usually choose to set your browser to remove and reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services. To opt out of interest-based advertising by advertisers on our Services, visit <http://www.aboutads.info/choices>.

### **Opting out of email marketing**

You can unsubscribe from our marketing email list at any time by clicking on the unsubscribe link in our emails or by contacting us using the details provided below. You will then be removed from the marketing email list – however, we will still need to send you

service-related emails necessary for the administration and use of your account. To otherwise opt-out, you may:

- Contact us using the contact information from Section 11
- Log into your account settings and update your preferences

## 9. Data breach

A privacy breach occurs when there is unauthorised access to or collection, use, disclosure or disposal of personal information. You will be notified about data breaches when SIA Trinat believes you are likely to be at risk of serious harm.

For example, a data breach may result in severe financial harm or harm your mental or physical well-being. Suppose SIA Trinat becomes aware of a security breach which has resulted or may result in unauthorised access, use or disclosure of personal information. In that case, SIA Trinat will promptly investigate the matter and notify the applicable Supervisory Authority within 72 hours after becoming aware unless the personal data breach is unlikely to risk the rights and freedoms of natural persons.

### **Controls for do-not-track features**

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track (“DNT”) feature or setting you can activate to signal your privacy preference and not to have data about your online browsing activities monitored and collected. No uniform technology standard for recognising and implementing DNT signals has been finalised. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of these Principles.

## 10. California

**In Short:** Yes, if you are a resident of California, you are granted specific rights regarding access to your personal information.

California Civil Code Section 1798.83, also known as the “Shine The Light” law, permits our Clients who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information from Section 11.

If you are under 18 years of age, reside in California, and have a registered account with the Services, you have the right to request the removal of unwanted data that you publicly post on the Services. To request the removal of such data, please contact us using the contact information provided below, and include the email address associated with your account and a statement that you reside in California. We will ensure the data is not publicly displayed on the Services, but please be aware that the data may be partially removed from our systems.

## 11. Contact details

The Client may contact SIA Trinat with any request, withdrawal of consent, update of data processing permission, data subject rights or complaint regarding the Processing of Personal Data. Contact details of SIA Trinat are available on our website: <https://trinat.lv>.

Based on the laws of some countries, you may have the right to request access to the personal information we collect from you, change that information, or delete it in some circumstances. The Client may contact the SIA Trinat appointed Data Protection Officer by sending an email to: [siatrinat@trinat.lv](mailto:siatrinat@trinat.lv) or sending a letter by post to: *Dammes iela 36-127, Riga, Latvia, LV-1069*, marked “Data protection officer”.

## 12. Validity and amendments of the Principles

SIA Trinat is entitled to unilaterally amend the Principles at any time in compliance with the Regulatory Legislation, by notifying the Clients of any amendments via our website, internet bank messages, text messages (SMS), or email, not later than 7 business days prior to the amendments entering into force.

These Principles are drafted in English and translated into Latvian and Russian. In the event of disputes, arguments, or claims of linguistic nature or concerning the interpretation, the version of these Principles in English is legally binding. Principles enter into force on July 1, 2023, and their latest version is available at the SIA Trinat headquarters and on the website: <https://trinat.lv>.