

## **Information regarding data processing and privacy and cookie policy on the website finture.com**

1. This Privacy Policy sets out the rules for the processing of personal data obtained through the website **finture.com**.
2. The Owner of the Service is Exorigo-Upos S.A. with its registered office in Warsaw (01-230), ul. Skierniewicka 10A, hereinafter referred to as "Exorigo-Upos". Exorigo-Upos together with FINTURE Sp. z o.o. and FINTURE AI Sp. z o.o. are entities connected capitally and organizationally, and cooperate with each other in providing comprehensive IT solutions. The companies have signed a co-administration agreement, the provisions of which are further described later in the policy.
3. Personal data collected by Exorigo-Upos together with FINTURE Sp. z o.o. and FINTURE AI z o.o. (hereinafter collectively referred to as "Joint Controllers)" through the Service are processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. on the protection of individuals with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation), also known as the "GDPR", the Personal Data Protection Act of 10 May 2018, the Telecommunications Law of 16 July 2004 and the Law on the provision of electronic services of 18 July 2002.
4. The joint administrators take special care to respect the privacy of customers (as defined below) visiting the Service.

### **Definitions**

1. **Personal data:** information about an identified or identifiable natural person (data subject).
2. **Data subject :** any natural person whose personal data are processed by the Joint Controllers in connection with his or her activities, e.g. a person with whom he has a contractual contract with one of the Joint Controllers or arequest to him in the form of an e-mail.
3. **Policy:** this Policy for the processing of personal data in companies of the Exorigo-Upos Capital Group.
4. **GDPR:** *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal

data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

5. **Service:** Website finture.com

6. **Joint controllers :** **The joint controllers of the personal data provided by you, i.e. the entities that jointly decide on the purposes and means of their processing,** are: Exorigo-Upos S.A., FINTURE Sp. z o.o. and FINTURE AI Sp. z o.o., hereinafter collectively referred to as Co-Administrators. Contact details for the Companies are shared: ul. Skierniewicka 10A, 01-230 Warszawa.

## **JOINT ARRANGEMENTS BETWEEN ADMINISTRATORS**

As part of the co-administration agreement, the Joint Administrators have agreed on the scope of their responsibility for fulfilling their obligations under the GDPR, in particular Exorigo-Upos S.A. is responsible for:

- for fulfilling the information obligations under the GDPR with regard to the disclosure referred to in Articles 13 and 14;
- carrying out activities aimed at promoting own products and services in order to attract new customers;
- notifying Violat data subjects in accordance with Article 34 of the GDPR;
- reporting personal data breaches to the supervisory authority in accordance with Article 33 of the GDPR;
- Exorigo-Upos S.A. is responsible for fulfilling your obligations under the GDPR with respect to the exercise of your rights.

## **INFORMATION ON THE PROCESSING OF PERSONAL DATA BY JOINT CONTROLLERS**

The joint controllers collect and process personal data in accordance with the relevant legal provisions, including in particular the GDPR, for the purpose of carrying out their economic activities.

The joint controllers shall comply with the principle of transparency in the processing of personal data. Data subjects are informed about the processing of data at the latest at the time of their collection and are also informed for the purpose and legal basis of their processing – e.g. when concluding a contract for the sale of goods or services.

The joint administrators ensure that the principle of minimization of personal data is respected in the Companies. The data are collected to the extent necessary for the indicated purpose of processing, and processed only for a minimum period of retention. In order to speed up and improve the service of their clients, the Joint Administrators collect personal data from them that is not necessary, for example, for the performance of the contract concluded with them – such as a telephone number or e-mail, only with their consent, and before collecting such data informs customers about the voluntary provision of such data.

The joint controllers shall ensure an adequate level of security and confidentiality of the personal data processed by them. In the event of an incident related to the security of personal data, as described above, Exorigo-Upos S.A. informs the data subjects of such an event in a manner consistent with the law.

### **CONTACT US ON MATTERS RELATED TO THE PROTECTION OF PERSONAL DATA**

The joint controllers have appointed a joint Data Protection Officer who can be contacted by:

1. e-mail [ochronadanych@exorigo-upos.pl](mailto:ochronadanych@exorigo-upos.pl),
2. by correspondence to Exorigo-Upos S.A. ul. Skierniewicka 10A, 01-230 Warszawa with the note "protection of personal data".

### **SECURITY OF PERSONAL DATA**

The procedures put in place by the Joint Controllers ensure an adequate level of confidentiality and integrity of the personal data processed by the Joint Controllers. Only persons who are adequately trained and authorised have access to personal data. The joint administrators shall use organisational and technical arrangements to ensure that all operations on personal data are recorded and carried out only by authorised persons.

The joint controllers shall take the necessary steps when selecting processors and other subcontractors so that the level of security of personal data with those entities is sufficient.

Co-administrators shall carry out an ongoing risk analysis and monitor the adequacy of the data security applied to the identified risks. If necessary, the Joint Administrations shall implement additional measures to enhance data security.

## **THE PURPOSES AND LEGAL BASIS FOR THE PROCESSING OF DATA BY THE JOINT CONTROLLERS**

The joint administrators shall collect information concerning natural persons carrying out economic or professional activities in their own name and natural persons representing legal persons or organisational units other than legal persons to whom the Law confers legal capacity, carrying out business or professional activities in their own name, hereinafter collectively referred to as "Clients". Customer personal data is collected in the case of:

**Contact via e-mail to answer your inquiry.** Legal basis - legitimate interest (Article 6(1)(f) GDPR), which is to provide an answer to the data subject.

**Determination, investigation and enforcement of claims.** In this case, some personal data provided by the Client in the context of the use of functionalities on the Website may be processed, such as: name, surname, data concerning the use of services, if the claims arise from the way in which the Customer uses the services, other data necessary to prove the existence of the claim, including the extent of the damage suffered. Legal basis - legitimate interest (Article 6(1)(f) GDPR), consisting in establishing, asserting and executing claims and defending against claims in proceedings before courts and other state authorities.

**Data collection in other cases.** In connection with its activities, each of the Joint Controllers also collects personal data in other cases – e.g. during business meetings, at industry events or through the exchange of business cards – for the purpose of establishing and maintaining business contacts. Personal data shall be provided on a voluntary basis in such cases. The legal basis for the processing in this case is the legitimate interest of the Joint Administrators (Article 6(1)(f) of the GDPR), consisting in networking in connection with the activities carried out. Personal data collected in such cases are processed only for the purpose for which they were collected.

Joint controllers shall ensure that the amount of data processed in correspondence complies with the principle of data minimisation and that only authorised persons have access to it.

When using the Website, additional information may be retrieved, in particular: the IP address assigned to the client's end device (e.g. phone, tablet, computer) of the Client or the external IP

address of the Internet service provider, domain name, browser type, access time, operating system type.

In order to market our own products and improve our services, navigation data may also be collected, including information about links and links in which they choose to click or other actions taken on our website, on the basis of the legitimate interest of the Joint Administrators (Art. 6 para. 1 lit. f GDPR), consisting in facilitating the use of services provided electronically and improving the functionality of these services.

The transfer of personal data to the Joint Controllers is voluntary in connection with the provision of services through the Service, but with the proviso that failure to provide the data specified in the form will prevent the provision of this service.

### **PERIOD OF PROCESSING OF PERSONAL DATA**

The period of data processing by the Joint Controllers depends on the purpose of the processing.

#### **Agreement**

Where the processing is necessary for the conclusion and performance of the contract, personal data will be processed until it is completed.

#### **Consent**

If the processing is carried out on the basis of consent, personal data are processed for its withdrawal. However, withdrawal of consent does not affect the lawfulness of processing based on consent prior to withdrawal.

#### **Legal provision**

Where the legal basis is a legal provision, the period of processing of personal data also results from specific provisions.

#### **Legitimate interest of the Joint Administrator**

In the case of data processing on the basis of the legitimate interest of the Joint Controllers, personal data are processed for a period enabling its implementation or to object effectively to the processing of data.

### **Protection against claims**

The period of data processing may be extended where the processing is necessary to establish, investigate or defend against possible claims and after that period only to the extent and to the extent required by law.

In the event of a retention period, personal data shall be deleted or anonymised without delay.

### **RECIPIENTS OF DATA**

Personal data may be transferred to entities from our group and subcontractors m.in. IT service providers – such entities process the data on the basis of a contract with one or more Joint Controllers and only in accordance with his instructions. Service providers are mainly established in Poland and other countries of the European Economic Area (EEA). In the event that your data is transferred outside the EEA, the Joint Controllers will apply appropriate legal safeguards, i.e. standard contractual clauses for the protection of personal data, approved by the European Commission.

Navigation data may be used to provide customers with better service, analyze statistical data and adapt the Service to customer preferences, as well as administer the Service.

In the event of a request to one of the Joint Controllers, your personal data may be made available to state authorities, in particular the organizational units of the Public Prosecutor's Office, the Police, the President of the Office for Personal Data Protection, the President of the Office for Competition and Consumer Protection or the President of the Office for Electronic Communications.

### **SOCIAL FUNCTIONS AND MARKETING**

Co-administrators process personal data of Users who visit the profiles of the Co-Administrators, which are carried out on social media (Facebook, LinkedIn). This data is processed only in connection with the conduct of the profile, including in order to inform users about the activities of the Joint Administrators and to promote various types of events, services and products. The legal basis for the processing of personal data is a legitimate interest (Article 6(1)(f) of the GDPR) in promoting its own brands.

### **COOKIE MECHANISM, IP ADDRESS**

Our website uses small files called cookies. They are stored on the end device of the visitor exorigo-upos.pl the website, if the web browser allows it. A cookie usually contains the name of the domain from which it originates, its "expiry time" and an individual, randomly selected number identifying the cookie. The information collected by such files allows you to compile general statistics of visits to our website.

Co-administrators use own cookies placed by the Website and cookies placed by third parties, approved by the Joint Controllers, including cookies of the Google Analytics tool.

List of cookies used by the website finture.com:

Co-Controllers cookies:

Category	Name	Shelf life	Purpose of storage
finture.com	_ <ga>#</ga>	do 2 lat	Used by Google Analytics to collect data on the number of times a user has visited the website as well as dates for the first and most recent visit.
finture.com	_ <ga< td=""> <td>do 2 lat</td> <td>Registers a unique ID that is used to generate statistical data on how the visitor uses the website.</td> </ga<>	do 2 lat	Registers a unique ID that is used to generate statistical data on how the visitor uses the website.

Cookies are used to:

1. analysis and research and auditing of viewership, and in particular to create anonymous statistics that help to understand how Customers use the Website, which allows to improve its structure and content;
2. ensuring the smooth functioning of the Service and adapting it to the needs of customers;
3. providing advertising services – presenting advertising messages tailored to the User's preferences.

Co-administrators do not use cookies to profile visitors to the websites referred to above.

Co-administrators use third-party cookies to collect general and anonymous static data through Google Analytics analytics tools (third-party cookie administrator: Google Inc. based in the USA).

The mechanism of cookies is safe for end devices used by customers of the website. In particular, this route does not prevent viruses or other unwanted software or malware from entering customers' endpoints. However, in their browsers, customers have the option to restrict

or disable the access of cookies to end devices. If you use this option, you will be able to use our website, in addition to functions that by their very nature require cookies.

The customer has the possibility to refuse the use of cookies in cases where the law is required to obtain such consent of the Administrator by pressing the button "<cancel>" on the screen informing about the use of cookies. The client of the website also has the ability to manage cookies by changing the settings on his device. Customer's consent will not be required when the storage or access to cookies is necessary in order to carry out the requested operation by the Client.

Here's how you can change the settings of popular web browsers regarding the use of cookies, including disabling their use:

1. Internet Explorer: <https://support.microsoft.com/pl-pl/help/17442/windows-internet-explorer-delete-manage-cookies>
2. Google Chrome:  
<https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=pl>
3. Mozilla Firefox: <https://support.mozilla.org/pl/kb/blokowanie-ciasteczek>
4. Apple Safari: <https://support.apple.com/pl-pl/guide/safari/sfri11471/mac>
5. Opera: <https://help.opera.com/pl/latest/security-and-privacy/>

Instructions for changing the settings of third-party cookies are specified in the policy issued by Google: <https://policies.google.com/?hl=pl>

Co-administrators may collect clients' IP addresses. An IP address is a number assigned to the end device of a visitor exorigo-upos.pl the website by an Internet service provider. The IP number allows access to the Internet. In most cases, it is dynamically assigned to the terminal device, i.e. it changes each time it connects to the Internet and is therefore generally treated as non-personal identifying information. The IP address is used by the Joint Administrators when diagnosing technical problems with the server, creating statistical analyses (e.g. determining which regions we record the most visits from), as useful information for administering and improving the service, as well as for security purposes and possible identification of incriminating server, unwanted automatic programs for viewing the content of our service.

## **RIGHTS RELATED TO THE PROCESSING OF PERSONAL DATA**

## **Rights of data subjects**

Data subjects have the following rights:

1. **Right to information about data processing** – on this basis, the person making such a request Finture provides information about the processing of his personal data, including, in particular, the purposes and legal grounds for processing, the scope of the data held, the entities to whom they are disclosed and the planned date of their deletion;
2. **Right to obtain a copy of the data** – on this basis Finture transmits a copy of the data processed concerning the person making the request;
3. **Right to rectification** – the Joint Controllers are obliged to rectify any inconsistencies or errors of the personal data processed and to supplement them if they are incomplete;
4. **Right to erasure** – on this basis, you can request the deletion of data whose processing is no longer necessary for the purposes for which they were collected;
5. **Right to restriction of processing** – in the event of such a request, the Joint Controllers shall cease to carry out operations on personal data, except for operations for which the data subject has consented and stored them, in accordance with the accepted retention rules, or until the reasons for the restriction of data processing cease (e.g. a decision of the supervisory authority authorising further processing of data will be issued);
6. **Right to data portability** – on this basis, in so far as the personal data are processed in connection with the concluded contract or consent, Finture will issue personal data provided by the data subject in a format that allows them to be read by a computer. It is also possible to request the transfer of this data to another entity – provided, however, that there are technical possibilities in this regard on the part of both Finture and that other entity;
7. **Right to object to the processing of data for marketing purposes** – the data subject may at any time object to the processing of personal data for marketing purposes, without the need to justify such objection;
8. **Right to object to other purposes of data processing** – the data subject may at any time object to the processing of personal data on the basis of the legitimate interest of the Joint Controllers (e.g. for analytical or statistical purposes or for reasons related to the protection of property). The opposition in this respect should state the reasons on which it is based;
9. **Right to withdraw consent** , – if the personal data are processed on the basis of the consent given, the data subject has the right to withdraw it at anytime, which, however,

does not affect the lawfulness of the processing carried out before the withdrawal of that consent;

10. **Right to a complaint** – if it is considered that the processing of personal data violates the provisions of the GDPR or other provisions on the protection of personal data, the data subject may lodge a complaint with the President of the Office for Personal Data Protection.

### **Making requests related to the exercise of rights**

An application for the exercise of the rights of data subjects may be submitted:

1. by traditional post to Finture Sp. z o.o. Skierniewicka 10A, 01-230 Warsaw with the note "Data Protection Officer" or
2. by e-mail to: [ochronadanych@exorigo-upos.pl](mailto:ochronadanych@exorigo-upos.pl)

Replies to notifications should be given within one month of receipt. If necessary to extend this period, Sp. z o.o. will inform the applicant of the reasons for such extension.

### **CHANGES**

In the event of a change in the applicable privacy policy, the above provision will be modified accordingly.

If you have any questions about the Privacy Policy, please contact: [ochronadanych@exorigo-upos.pl](mailto:ochronadanych@exorigo-upos.pl)

**Date of the last modification:** 10/20/2022