



# Whistleblowing

# Whistleblowing

Liferay has established a whistleblowing channel.

If you believe there have been any illegal, fraudulent or unethical activities within Liferay you can report these in a confidential or anonymous manner.

You can access the whistleblowing channel [whistleblowersoftware.com/secure/external](https://whistleblowersoftware.com/secure/external).

You can either report in writing or verbally. The usage of the channel is intuitive.

The whistleblowing channel is guided by the principles of Confidentiality, Transparency, Objectivity, Honesty, Respect and Independence. Whistleblowers are protected from retaliation. It also allows for anonymous reporting.

The whistleblowing channel uses a secure external digital tool, the “Whistleblower Software” (<https://whistleblowersoftware.com/es>). It is a software with the highest levels of information security to ensure anonymity and protection to the whistleblower and it complies with data protection and security requirements, such as Schrems II or end-to-end encryption.

Here is an excerpt of what is reportable, among others:

- Harassment, hostile or offensive behavior;
- Actions related to possible irregularities in the interaction with suppliers, vendors and/or purchases;
- Actions related to public and private corruption;
- Misappropriation and diversion of resources;
- Money laundering;
- Accounting irregularities and inaccuracies;
- Conflict of interest;
- Undue commitments with third parties;
- Falsification of documents, contracts, reports or records;
- Violation of employee rights;
- Violations of information security;
- Any behavior that would violate applicable local or European law or regulations or Liferay’s internal policies and procedures.

# Details on Principles that govern the channel

The whistleblowing channel is based on the following principles:

## 1. Principle of Independence.

Liferay applies the utmost objectivity and independence, and establishes the corresponding mechanisms in order to avoid the concurrence of possible conflicts of interest.

## 2. Principle of Confidentiality.

Liferay takes great care in protecting confidentiality. Liferay establishes the maximum confidentiality of the reports that may be received, together with the data contained in them.

The above does not affect the data that must be disclosed to the authorities because of the magnitude of the facts or judicial or administrative proceedings that so require.

## 3. Principle of Tolerance and Respect.

Liferay, rejects any conduct which may be against its principles and the current legislation. In accordance with this rejection, the obligation to communicate the knowledge of any misconduct is imposed.

## 4. Principle of Objectivity and Honesty.

The actions that order the procedure will be governed in all cases by the principles of absolute objectivity and maximum honesty.

Reporting has to be made in good faith. Good faith means that the reporter had reasonable grounds to believe that the information provided regarding the suspicious acts or omissions was true at the time of reporting.

## 5. Prohibition of Retaliation.

It is absolutely forbidden to take any action against any person who uses the whistleblowing channel. Any action which involves retaliation or a negative consequence, on the grounds of having made a report in a proper manner and subject to the present procedure, are rejected by Liferay.

The foregoing is, notwithstanding of those measures, that may be appropriate, whenever the internal investigation unequivocally shows that the report is false or malicious.

## 6. Anonymous Reporting

Reporting can be done openly or anonymously.

An anonymous report, however, might hinder the possibility of investigation as information shared might be insufficient.

## 7. Whistleblower's Protection

The whistleblowing channel, through the external Software, has the necessary protections to maintain the security of communications and confidentiality of the information and documentation provided, if any, by the whistleblower.

The whistleblowing channel will be governed by the principle of maximum confidentiality, adopting any measures necessary to ensure that no retaliation is taken against the whistleblower who has acted in good faith.

## 8. Applicability

This applies to the companies (i) Liferay S.L., with registered address at Paseo de la Castellana, 280 Planta 1ª. Modulo B 28046 - Madrid (Spain) and (ii) Liferay Hungary Kft., with registered address at 1138 Budapest Madarász Viktor Utca 47. A-b (Hungary) (herein "Liferay"), in compliance, respectively, with the Spanish law "Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción" and the Hungarian regulation "Act XXV de 2023", which transpose the EU Directive 2019/1937 (Whistleblower Directive).

## 9. Privacy Notice

To the extent the Whistleblower reports non-anonymously, Liferay will process your personal data (your name and, optionally, your telephone number) and, in any case, the other personal data included in the report, based on our legal obligations under the applicable whistleblowing laws.

The processing of the personal data will be carried out for the sole purpose of fulfilling legally established obligations, including fraud prevention, investigating the complaint made and taking the necessary actions based on the result of the mentioned investigation.

We will share the personal data, as might be required, with the legal advisors, relevant authorities, and service providers.

The personal data will remain in the EEA. If in the course of the investigations it is necessary to transfer your personal data to third countries, Liferay will take the appropriate measures provided in the GDPR as (i) contractual arrangements with the recipient of the personal data, using, for example, the Standard Contractual Clauses

approved by the European Commission or (ii) transferring the data to a third country offering an adequate level of protection through a European Commission decision (“Adequacy Decision”).

You have the following rights in relation to our processing of your personal data:

- Right to access: You can ask us to give you information about whether or not your personal data is processed, and if yes, certain further details, such as with which entities your personal data has been shared;
- Right to rectification: if you deem that your data is falsely recorded in our systems, you can ask to have that rectified;
- Right to erasure: in certain situations (especially if the processing of your personal data is based on consent provided by you) you can ask that we delete, block or anonymize personal data related to you. However, we may oppose this request (especially if we have a legal obligation to store your personal data).
- Right to object to the processing of personal data: If we process your personal data based on our legitimate interest, you have the right to object against these types of data processing activities..
- Right to refuse consent: if we ask you to provide consent, you should be aware that you can refuse to provide consent, without any major detriment, except eventually inconvenience. We will inform you in each particular case of the available alternatives and the consequences.
- Right to withdraw consent: If you gave your consent to us, you are free to withdraw that at any time and without any conditions. That case we will not process your personal data in the future for the reason we sought your consent for.
- Right to request restriction of processing: You also have the right to restrict the processing of personal data: there are situations (for example if you contest the accuracy of your personal data and we are verifying the accuracy of the data) in which you have the right to ask for the restriction of the processing of your personal data. If this right is exercised, we can only store your personal data, but we cannot make any other action on it (e.g. we cannot create statistics using it).
- Right to data portability: Under certain circumstances you can request us to enable portability of your data to another service or product provider.

Further to the above, if you feel that we have breached the applicable data protection laws, you have the right to lodge a complaint with the data protection supervisory authority of your country. If you are based in the EU, you can find the competent authority and the contact details here:

[https://edpb.europa.eu/about-edpb/about-edpb/members\\_en](https://edpb.europa.eu/about-edpb/about-edpb/members_en).

For any questions or requests relating to this Privacy Notice or handling of your personal data by Liferay, please contact us as at: [dataprotection@liferay.com](mailto:dataprotection@liferay.com)



Liferay makes software that helps companies create digital experiences on web, mobile and connected devices. Our platform is open source, which makes it more reliable, innovative and secure. We try to leave a positive mark on the world through business and technology. Hundreds of organizations in financial services, healthcare, government, insurance, retail, manufacturing and multiple other industries use Liferay. Visit us at [liferay.com](https://www.liferay.com).

© 2023 Liferay, Inc. All rights reserved.