

# Whistleblowing Policy

---

*Policy adopted by the Board of Directors of Plejd AB 2023-12-05*

Plejd AB (“Plejd” “we” or “us”) works actively to create a safe and secure environment for everyone who comes into contact with us, whether you are an employee, job seeker, consultant or supplier. We also work continuously to prevent any irregularities or malpractices in our business and it is important to us that you feel safe to report any misconducts that may occur.

You have the right to whistleblow if you suspect that any misconduct of public interest or violations of the law has occurred at Plejd. Whistleblowing simply means that you bring the problem to our attention (so that we can take action) and that you are protected.

This policy contains information about whistleblowing and answers the following questions;

- Who has the right to whistleblow?
- Which misconducts can you whistleblow about?
- Which misconducts can you not whistleblow about?
- How do you whistleblow?
- What should (and should not) be included in your whistleblowing report?
- What happens when you whistleblow?
- Which rights do you have as a whistleblower and how are you protected?
- How do we handle your personal data?

You can reach us by sending an email to [whistleblower@plejd.com](mailto:whistleblower@plejd.com) if you have any additional questions about whistleblowing that have not been answered in this Policy. You can also use the chat function in our whistleblowing platform after you have filed a report.

## Who has the right to whistleblow?

You may whistleblow if you belong, or have belonged, to any of the following groups:

- Plejd employee
- Plejd intern
- Plejd consultant
- Job applicant at Plejd
- Plejd supplier or subcontractor
- Plejd shareholder (if you are active in the company)
- Plejd board member
- Plejd advisor

## What you may whistleblow about?

You may whistleblow if you have reason to believe that any misconduct of public interest occurs, has occurred or will occur within Plejd. This means that you may report information regarding any serious misconduct which concerns the public if there is a legitimate interest that the misconduct comes to light.

You may also whistleblow if you have reason to believe that any misconduct which violates certain EU-laws occurs, has occurred or will occur within Plejd.

It can be a case of misconduct based on someone doing something, or failing to do something that they should have done. It does not matter whether the act of misconduct has arisen from someone's deliberate action or by accident. Furthermore, the misconduct does not have to be current or ongoing, it can also apply to completed and fully exposed misconducts.

Here are some examples of what you may whistleblow about:

- Financial crimes, such as accounting or tax offences,
- Harassment, such as bullying or sexual harassment,
- Discrimination against individual employees,
- Serious shortcomings in the working environment,
- Serious breaches of the GDPR,
- Serious deficiencies of information security,
- Serious deficiencies in workplace security,
- Serious deficiencies in consumer protection,
- Corruption or bribery,
- Serious deficiencies in matters relating to the fundamental interests of Plejd.

## What should I not whistleblow about?

We want you to feel safe to bring up any issues that you have or notice at Plejd so that we can take action and keep getting better. However, it is important to understand that the whistleblowing channels and our procedure for whistleblowing is intended for such serious misconducts as noted above.

You should not whistleblow on matters relating to your own employment relationship, such as dissatisfaction with your pay progression or being too busy at work. Such issues should instead be raised with your manager or Team HR.

Furthermore, whistleblowing must be within the scope of Plejd's operations, which means that incidents of a purely private nature or that occur within another company should not be reported to us.

## How do I whistleblow internally?

You have the right to whistleblow either in writing, orally or at a physical meeting, as further described below.

You can whistleblow to us by filing a report in writing through our whistleblowing platform. You can choose to report anonymously through the whistleblowing platform by not filling in your name, email or phone number. If you choose to fill in your name, email or phone number, your identity will only be known to the persons that have been authorized to handle whistleblowing reports for Plejd.

You can request a physical meeting through our whistleblowing platform or by sending an email to [whistleblower@plejd.com](mailto:whistleblower@plejd.com) to present your report on-site with us. We will set up the meeting as soon as reasonably possible. We may record our meeting, if you agree to it. Otherwise, we will draw up minutes that you will be given the opportunity to review and then sign.

You can also whistleblow orally by recording an audio message and upload your file to the whistleblowing platform.

When you have filed your report you will receive a case code that will give you access to the relevant case in the Whistleblowing Platform. It is not possible to access the Whistleblowing Platform without the case code so make sure you save it and keep it safe. You can also upload supporting files once the case has been submitted. Be aware that if you upload files they might contain metadata such as location that can reveal your identity.

You can access our whistleblowing platform by going to the following page: [Plejd's Whistleblowing Platform](#).

## Public whistleblowing

You can also whistleblow to public authorities, provided that the misconduct or violation of the law falls within their area of responsibility. Contact details to the competent authorities and a description of their respective responsibilities are available at the following website: [Public whistleblower channels](#)

## What should (and should not) be included in the report?

Your report should be in either English or Swedish and as detailed as possible to enable us to consider whether a follow-up action is needed. If you have documents or pictures to support your report, please attach them.

We ask you to leave out any information that is not relevant to the misconduct concerned. Furthermore, we ask you not to submit sensitive personal data, such as information about someone's health, sexual orientation or trade union membership, unless it is absolutely necessary for the purpose of reporting the misconduct in question.

## What happens afterwards?

The reports will be received by authorized members of the board of directors of Plejd. After you have reported a misconduct they will get back to you with a confirmation of receipt within seven days, unless you have waived further information, submitted a report without

providing any contact details or if they have reason to believe that such confirmation would reveal your identity.

We will thereafter get back to you within three months with a comprehensive description of the actions taken in response to your report through the whistleblowing platform.

Usually, an investigation is first made into the correctness of the reported claims. The follow-up investigation will be carried out by an authorized external investigator. We may then decide not to take action, or refer the matter to another department within Plejd for further action.

## How am I protected?

Provided that you meet the criterias above, you will be protected by law. If you, the reporter, are subject to confidentiality, you will not be held responsible for breaching your confidentiality provided that you had reasonable grounds to believe that the reporting of the information was necessary to disclose the reported misconduct.

You are further protected against reprisals, which includes any action that results in any form of harm to you as a whistleblower. This means for example that you will not be suspended, dismissed or denied promotion and that you are protected from disciplinary action, termination of probation, damage to your reputation or termination of your contract (if you are a supplier) or other adverse action. Plejd will also ensure that you are protected from any kind of informal reprisals, such as not being invited to important meetings or being given less qualified work after filing a report. The protection also applies to others who assist you or companies you own, or that you are associated with.

Your report will be treated anonymously, if you choose, and the person handling the follow-up is bound by a legal obligation of confidentiality.

## How is my personal data handled?

We may process and retain personal data from the report for up to two years after the follow-up case has been closed. If there is personal data in the report that is not relevant, it will be deleted.

We process your personal data due to the regulations in the Swedish Whistleblowing Act (Sw: lag (2021:890) om skydd för personer som rapporterar om missförhållanden).

If you would like additional information about how Plejd processes personal data and how you can exercise your rights, please refer to our privacy policy below.

# Privacy Policy for Whistleblowers

## Why do we have a privacy policy?

While handling your report Plejd AB (“Plejd”, “we” or “us”) care about your privacy. Therefore, we always make sure to protect your personal data in the best possible way.

In this privacy policy we want to inform you as a whistleblower how we process your personal data. Below is a summary of the purposes for which we process your personal data. Further down in this privacy policy we explain in detail what personal data we process, why we need to process it and the legal basis for our processing of your personal data. We also explain the rights you have in relation to our processing of your personal data.

If you have any questions regarding our processing of your personal data or if you wish to exercise your rights under the data protection legislation, please contact us via our email address [info@plejd.com](mailto:info@plejd.com) or give us a call on +46 (0) 10 207 89 01.

## Our processing in summary

In summary we process your personal data (such as your contact details and other information that you provide in your report) for the following purposes:

- to communicate with you as a whistleblower when you have filed a report;
- to administer the follow up investigation;
- to inform you of the conclusions of the investigation and the actions taken as a result of the investigation.

## Who is responsible for processing your personal data?

Plejd AB, registration number 556790-9477, with phone number +46 (0) 10 207 89 01 and email address [info@plejd.com](mailto:info@plejd.com) is responsible for the processing of your personal data (the controller).

## From where do we collect your personal data?

When you file a whistleblowing report through our whistleblowing platform you may provide us with information about yourself, such as your name, contact details and other information included in your report.

## Are you required to provide personal data to us?

You are not required to provide personal data to us. Please note that you may file your report anonymously by not filling out your name, email or phone number.

## Who will have access to your personal data?

The board of directors of Plejd shall authorize at least two of their members and/or an external party which shall be responsible to receive the whistleblowing reports that are submitted (the “**Authorized Recipients**”). After receiving a report the Authorized Recipients shall ensure that an external party is appointed to manage the follow-up investigation (the “**External Investigator**”). Only the Authorized Recipients and the External Investigator will have access to your personal data. They are bound by a legal obligation of confidentiality. The Authorized Recipients and the External Investigator will report directly to the board of directors of Plejd.

## For how long will we store your personal data?

We will store your personal data for as long as we have an ongoing investigation regarding your report. Thereafter we will store your personal data for as long as necessary but not longer than a period of two years after the investigation is closed. Personal data which are manifestly not relevant for the handling of a specific report will however be deleted without undue delay if accidentally collected.

## How do we share your personal data and why?

Your personal data will be processed by us through the Authorized Recipients. However, in order to carry out the investigation we will share your personal data with a law firm that is appointed as the External Investigator.

Furthermore, we share your personal data with our subprocessor AlexisHR AB (“AlexisHR”) that is the supplier of our whistleblowing platform. We do that to administer your report and to store the information that you provide in your report. Please note that the information you provide will be encrypted and that AlexisHR will not be able to gain access to such information.

*Please contact us if you want to know more about who we share your personal data with. You will find our contact details in the beginning of this privacy policy.*

## Processing of your personal data outside the EU/EEA

We always strive to process your personal data within the EU/EEA.

However, in some cases when using AlexisHR we will transfer your personal data outside the EU/EEA because AlexisHR processes your personal data outside the EU/EEA. Such transfers only take place in accordance with the General Data Protection Regulation (“GDPR”). We only transfer your personal data outside the EU/EEA when we can ensure an adequate level of protection of your personal data. In all situations where we transfer your personal data outside the EU/EEA it is based on one of the lawful grounds mentioned below:

- The EU Commission has decided that the recipient country in question ensures an adequate level of protection;

- If your personal data is transferred to the United States, the transfer can be based on the adequacy decision of the European Commission "EU-US Data Privacy Framework", but only if the recipient has joined the framework;
- We have established appropriate safeguards for the transfer of personal data by using the standard data protection clauses approved by the Commission. Please note that if a transfer is based on this lawful ground you have the right to obtain a copy of such standard data protection clauses by contacting us; or
- You have given your explicit consent for the transfer of your personal data or another lawful basis for the transfer of your personal data outside the EU or EEA exists.

*Please contact us if you want to know more about how we transfer your personal data or if you want more information about the appropriate safeguards we have in place to protect your personal data. You will find our contact details in the beginning of this privacy policy.*

## Which rights do you have in relation to our processing of your personal data?

According to the GDPR you have several rights in relation to our processing of your personal data, which are set out below.

*If you have any questions regarding these rights or if you want to exercise any of your rights, please contact us. You will find our contact details in the beginning of this privacy policy.*

### Right to information and access

You have the right to obtain confirmation on whether or not we process your personal data. If we process your personal data, you also have a right to receive information about how we process the personal data and to receive a copy of your personal data.

### Right to rectification

You have a right to have inaccurate personal data corrected and to have incomplete personal data completed.

### Right to erasure (right to be forgotten) and restriction of processing

You have the right to have your personal data erased in certain cases. This is the case e.g. when the personal data is no longer necessary for the purposes for which it was collected or otherwise processed and where we process your personal data on the basis of our legitimate interest and we find, following your objection (see below under Right to object), that we do not have an overriding interest in continuing to process it.

You also have the right to request that we restrict our processing of your personal data. For example, when you question the accuracy of the personal data, when you have objected to our processing of your personal data based upon our legitimate interest, or where the

processing is unlawful, and you oppose the erasure of your personal data and instead want us to restrict our processing.

## Right to data portability

Under certain circumstances you have the right to be provided with personal data (concerning you) that you have provided to us, in a structured, commonly used and machine-readable format. You also have a right to in certain instances have such personal data transferred to another controller, where technically feasible.

## Right to object

You have the right to object to our processing of your personal data when the processing is based on legal basis “legitimate interest”. The situations when we base our processing on our legitimate interest are stated in the below charts and you can read more about our balancing of interest assessments in the end of this privacy policy. In some instances, we may continue to process your personal data even if you have objected to our processing. This can be the case if we can show compelling legitimate reasons for the processing that outweigh your interests or if our processing is necessary for the purpose of establishing, exercising or defending against legal claims.

## Right to lodge a complaint to a supervisory authority

You have the right to lodge a complaint to a supervisory authority concerning our processing of your personal data.

Such a complaint can be filed to the authority in the EU/EEA member state where you live, work or where the alleged infringement of applicable data protection legislation has occurred. The Swedish supervisory authority is

## Detailed description of how we process your personal data

The charts below describe in detail why we process your personal data, the categories of personal data we process, the legal basis for our processing and how for how long we will store your personal data.

To receive the rapport, get back to you with a confirmation of receipt and communicate with you.		
Why we process your personal data	Personal data processed	Legal basis



<ul style="list-style-type: none"> <li>• To receive the report.</li> <li>• To get back to you with a confirmation of receipt (unless you have waived further information or submitted a report without providing you contact details).</li> <li>• To inform you of updates and communicate with you if we need to ask you further questions regarding your report.</li> <li>• To get back to you with a description of the actions taken in response to your report.</li> </ul>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Email</li> <li>• Phone number</li> </ul>	<p>The processing is necessary for us to comply with the legal obligations set forth in the Swedish Whistleblowing Act (Sw: lag (2021:890) om skydd för personer som rapporterar om missförhållanden).</p>
<p>Retention: We will store your personal data for as long as we have an ongoing investigation regarding your report and for a period thereafter if necessary but not for a longer period than two years after the investigation is closed.</p>		

During and after our follow up and investigation if you have filed a report		
Why we process your personal data	Personal data processed	Legal basis
<ul style="list-style-type: none"> <li>• To receive, follow up, investigate and if necessary take action regarding the information included in your report.</li> </ul>	<ul style="list-style-type: none"> <li>• Personal data included in the report.</li> <li>• Personal data collected during the investigation.</li> </ul>	<p>The processing is necessary for us to comply with the legal obligations set forth in the Swedish Whistleblowing Act (Sw: lag (2021:890) om skydd för personer som rapporterar om missförhållanden).</p>
<p>Retention: We will store your personal data for as long as we have an ongoing investigation regarding your report and for a period thereafter if necessary but not longer than a period of two years after the investigation is closed. Personal data which are manifestly not relevant for the handling of a specific report will be deleted without undue delay if accidentally collected.</p>		

If we need to report a misconduct to the authorities		
Why we process your personal data	Personal data processed	Legal basis
<ul style="list-style-type: none"> <li>• If necessary to report misconducts to the competent authority.</li> <li>• If necessary to use the personal data as evidence in legal proceedings.</li> </ul>	<ul style="list-style-type: none"> <li>• Personal data included in the report.</li> <li>• Personal data collected during the investigation.</li> </ul>	<p>The processing is necessary for us to comply with the legal obligations set forth in the Swedish Whistleblowing Act (Sw: lag (2021:890) om skydd för personer som rapporterar om missförhållanden) or as set forth in other applicable legislation.</p>
<p>Retention: We will store your personal data for as long as we have an ongoing investigation regarding your report and for a period thereafter if necessary but not longer than a period of two years after the investigation is closed. Personal data which are manifestly not relevant for the handling of a specific report will be deleted without undue delay if accidentally collected.</p>		