



# Whistleblower Reporting - How is my personal data processed?

## REGEL/RIKTLINJE

*This document has been translated from its original Swedish version*

Peab Group values your privacy and always strives to protect your personal data in the best possible way and comply with all applicable laws and regulations regarding data protection. We are open and transparent in our processing of your personal data when you report a misconduct (when you "blow the whistle") to the whistleblowing contacts in the various Peab companies, as well as through our whistleblowing tool on the intranet and the external website <https://report.whistleb.com/sv/Peab>.

If you do not have access to your company's whistleblowing contacts via the intranet, we ask you to request this directly through the whistleblowing tool. For privacy reasons, Peab has chosen not to publish the names of whistleblowing contacts on external websites. In the whistleblowing tool, all communication can be anonymous.

The Whistleblower Act (SWE: Act (2021:890) on the protection of persons reporting misconduct) contains specific rules on the processing of personal data. The rules in the Whistleblower Act complement the provisions on the processing of personal data in the General Data Protection Regulation (GDPR).

Below is an account of how the Peab companies within the Peab Group process personal data in the context of whistleblowing.

1. Who is the data controller? .....	2
2. On what legal grounds are your data processed? .....	2
Legal obligation .....	2
Consent .....	2
Legitimate interest .....	3
3. What are the requirement of processing personal data? .....	3
4. Do you have any questions about Peab's processing of your personal data? .....	3
5. Impact assessment, privacy and confidentiality .....	3
6. Where and how are my personal data processed? .....	4
a) Third-party tool .....	4
b) Specifically selected whistleblowing contacts in your company .....	4
c) Peab AB's Whistleblowing Council .....	4
d) Can be expanded to a wider circle .....	5
e) Who follows up on the case? .....	5
7. What happens to the personal data if i report orally? .....	5
8. What personal data do we process? .....	5
9. Are all personal data stored? Accuracy .....	5
10. Storage, deletion .....	5
11. Transfer of personal data to third countries .....	6
12. Your rights .....	6
13. Changes to this information .....	6

#### **1. WHO IS THE DATA CONTROLLER?**

The assessment of which company is the data controller for a specific processing of personal data is made based on the factual circumstances in each individual case. Different companies within the Peab Group may therefore be data controllers for the processing of your personal data. Which Peab company is the data controller for the processing depends on the Peab company you report/whistle about, are employed by, or have another relationship with.

Peab AB is a data processor for all companies except itself, where Peab AB has its own data controller responsibility. Peab AB has appointed a Whistleblowing Council, which handles reports of misconduct ("whistleblowing") on behalf of the entire Group.

#### **2. ON WHAT LEGAL GROUNDS ARE YOUR DATA PROCESSED?**

##### **Legal obligation**

The Peab company has an obligation under the Whistleblower Act to have reporting channels and procedures for reporting and follow-up on a whistleblower report. Therefore, the processing of personal data by the Peab company will be based on the necessity of processing personal data in order to fulfill a legal obligation incumbent on the Peab company.

##### **Consent**

Consent as a legal basis for processing personal data is only used when recording whistleblowing if requested by an individual. Consent is obtained in advance.

### **Legitimate interest**

It may be permitted to process personal data based on a legitimate interest. In such cases, the processing must be necessary for legitimate interests that outweigh the data subject's interest in the protection of their personal data.

### **3. WHAT ARE THE REQUIREMENT OF PROCESSING PERSONAL DATA?**

In Peab's specific whistleblowing function, the Whistleblowing Council (the Council) initially receives reports, and the Peab company's designated representatives, the whistleblowing contacts, have direct contact with the whistleblower. Whistleblowing reports can be submitted orally, in writing via letter/email/third-party tool, or in a physical meeting.

Personal data may only be processed if the processing is necessary for a follow-up case.

In connection with the receipt of reports, the reports are documented, meaning that records are kept, while oral reporting needs to be recorded or documented in minutes.

The whistleblowing function also needs to confirm receipt to the whistleblower. Subsequently, actions need to be taken to assess the accuracy of the allegations made in the report. This may involve contacting other individuals to confirm or refute the allegations, such as witnesses and experts.

Finally, the whistleblowing function needs to provide feedback to the reporting individual on the conducted investigation and the conclusions drawn from the investigation.

### **4. DO YOU HAVE ANY QUESTIONS ABOUT PEAB'S PROCESSING OF YOUR PERSONAL DATA?**

If you have any questions about the Peab companies' processing of your personal data or if you wish to exercise your rights under the General Data Protection Regulation, you are welcome to contact us by letter or email. Peab AB, Attn: Peab Data Protection Coordinator, Margretetorpsvägen 84, 269 73 Förslöv. You can also contact us by email at [gdpr@peab.se](mailto:gdpr@peab.se).

Learn more about your rights (access, rectification, erasure, restriction, objection) in Peab's handling of personal data at <https://peab.se/gdpr/>.

### **5. IMPACT ASSESSMENT, PRIVACY AND CONFIDENTIALITY**

In connection with Peab's investigation of the processing of personal data related to whistleblowing, it was identified that there may be different privacy risks. These are primarily associated with the processing of personal data in follow-up cases.

It is evident that the personal data processed will often be of a sensitive nature. The data may include established or suspected crimes and other violations of laws and regulations allegedly committed by identified individuals, such as financial crimes, corruption offenses, occupational safety offenses, discrimination, and harassment.

To ensure proper processing of personal data, Peab has implemented appropriate technical and organizational security measures. This includes:

- Peab company has a legal basis for the processing of personal data (lawfulness, paragraph 2) and is accurate (paragraph 9).
- It is clear and transparent how Peab company processes personal data. Peab company also shows how an individual can exercise their rights, such as how to correct incorrect information and how to have personal data erased (transparency, preamble, and paragraph 4).
- Peab collects personal data for specific, explicitly stated, and legitimate purposes (purpose limitation, paragraph 3).

- To prevent data from being disseminated, whistleblowing reports are handled only by a limited group of individuals with specific internal procedures, instructions, and guidelines (privacy and confidentiality, paragraph 6).
- Data is processed only to the extent necessary to handle a follow-up case (data minimization).
- Peab retains personal data for as long as necessary for the purpose of the processing of personal data (storage and deletion, paragraph 10).
- The technical measures implemented by Peab include encryption, pseudonymization, backup, and antivirus protection (paragraph 6).

## **6. WHERE AND HOW ARE MY PERSONAL DATA PROCESSED?**

The processing of personal data in the reporting channels is managed by a limited group of individuals. In some cases, personal data may need to be shared with individuals who are not part of this group, such as the police or prosecutor, Peab's security department, HR department, or legal department. Personal data may also need to be shared internally within the organization to address misconduct.

To ensure the protection of your personal data and safeguard your fundamental rights, Peab has implemented measures to restrict access to personal data. Only authorized individuals or entities have access to the personal data, and only to the extent necessary to perform their duties related to whistleblowing.

Personal data that is not relevant to the handling of a report is not collected, and any inadvertently collected personal data is deleted as soon as possible.

The personal data is processed manually, and no automated decisions are made.

### **a) Third-party tool**

Your whistleblowing is handled through a third-party tool owned by an external provider, WhistleB (<https://whistleb.com/>). WhistleB ensures the anonymity of the whistleblower if they choose to remain anonymous and the secure handling of reports submitted through the system. Peab AB has established a data processing agreement with WhistleB to ensure the protection of personal data.

Reports and subsequent communication between Peab and the reporter are encrypted and protected with passwords. Within Peab, no one has the ability to ascertain the identity of an anonymous reporter.

### **b) Specifically selected whistleblowing contacts in your company**

Within the Peab Group, there are specifically selected whistleblowing contacts in all companies with more than 250 employees. These whistleblowing contacts have specific confidentiality obligations regarding the handling of whistleblowing reports. Through specific agreements between the companies, instructional documents, and confidentiality agreements, these companies allow whistleblowing reports to be processed at the group level by Peab AB. In companies with fewer than 250 employees, Peab AB is responsible for handling whistleblowing reports.

### **c) Peab AB's Whistleblowing Council**

Whistleblowing reports within Peab AB are handled by Peab's Whistleblowing Council. The Council consists of competent individuals with professional qualifications and expertise in data protection legislation, privacy, and whistleblowing management according to GDPR and the Whistleblower Act. The Council consists of Peab AB's Chief Legal Counsel, Corporate Governance and Compliance, Group Security Manager (investigation officer), Group HR Manager, and Corporate Legal Counsel, Compliance and Corporate Governance.

Only the whistleblowing contacts in the company through which you report, if available, and the Council are allowed to handle the initial processing of a whistleblowing report. This means they receive the report, have contact with the reporter, and take the necessary actions to assess the accuracy of the report. If further investigation or collaboration with other units within Peab is deemed necessary, the case may be delegated to appropriate individuals within the organization.

**d) Can be expanded to a wider circle**

If necessary, access to personal data may be expanded to a broader group to enable a more comprehensive investigation. However, the processing of personal data is limited to what each individual needs to fulfill their duties related to the whistleblowing. If the Council considers it necessary to disclose information about the investigated allegations for further actions, we will provide feedback to you through the whistleblowing tool. If you have chosen to remain anonymous, we will not attempt to investigate your identity or identify any other individuals involved in the case.

**e) Who follows up on the case?**

The whistleblowing contacts in your Peab company or, in some cases, the Council provide feedback on the follow-up to you, which is done encrypted and anonymized through the whistleblowing tool.

It is important to note that the individual specifically designated to handle a follow-up case is not allowed to disclose information that may reveal your identity or the identity of any other individuals involved in the case.

**7. WHAT HAPPENES TO THE PERSONAL DATA IF I REPORT ORALLY?**

If you choose to report orally, it will be documented through a recording or a prepared protocol. Recording means that the entire conversation is recorded to be saved in a durable form. Protocol means a written account of the information provided, covering the relevant details of the report.

To allow for recording, your consent is required. Such consent must be obtained before the recording starts.

You will be given the opportunity to review, correct, and approve a transcript or protocol through your signature.

**8. WHAT PERSONAL DATA DO WE PROCESS?**

The processing of personal data is limited to the personal data that is strictly and objectively necessary to verify the legitimacy of the reported whistleblowing. Only relevant and necessary information is collected, and any collected information that is not relevant is deleted as soon as possible.

**9. ARE ALL PERSONAL DATA STORED? ACCURACY**

Peab's processing of personal data is fair, reasonable, and proportionate to the whistleblowing. The processing of personal data must always be proportionate to the benefits it entails.

Personal data that is clearly not relevant to the handling of a specific whistleblowing report must not be collected, and if collected by mistake, it will be deleted as soon as possible.

Peab takes into account what processing of personal data the data subjects can reasonably expect.

The processing of personal data should be understandable and clear to the data subjects and should not be carried out in a hidden or manipulative manner.

**10. STORAGE, DELETION**

The personal data is stored in WhistleB's encrypted and password-protected tool (with two-factor authentication) as well as in a local folder with strict user permissions controlled by the Council. Personal data in a follow-up case is only processed for as long as necessary for the purpose and is not retained for more than two years after the case is closed. Storage and deletion are carried out in accordance with applicable laws and regulations.

### **11. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES**

Peab processes all personal data, when it comes to these reports, within the EU and the European Economic Area (EEA).

### **12. YOUR RIGHTS**

Under the General Data Protection Regulation, you have certain rights regarding the processing of your personal data. These rights include:

**Right of access:** You have the right to obtain information about which of your personal data is being processed and how it is processed.

**Right to rectification:** If your personal data is incorrect or incomplete, you have the right to request its correction.

**Right to erasure:** Under certain circumstances, you have the right to request the erasure of your personal data.

**Right to restriction of processing:** You can request the restriction of the processing of your personal data under certain circumstances.

**Right to data portability:** If technically feasible, you have the right to have your personal data transferred to another data controller.

**Right to object:** You have the right to object to the processing of your personal data under certain circumstances.

**Right not to be subject to automated decision-making:** You have the right not to be subject to decisions based solely on automated processing, including profiling, if such decisions have significant legal effects on you.

If you wish to exercise any of your rights or if you have questions or complaints about the processing of your personal data, you are welcome to contact Peab via mail or email.

### **13. CHANGES TO THIS INFORMATION**

This information may be updated from time to time to reflect any changes in our processing of personal data or changes in applicable legislation.