

SPEAK-UP LINE - PRIVACY NOTICE IN RELATION TO WHISTLEBLOWING

1. INTRODUCTION

Whistleblowing made through, or other information relating to, the reporting system (“Speak Up Line”) and procedures implemented within Billerud will contain personal data processing. Billerud AB or one of its subsidiary companies is the data controller in respect of the processing of such personal data.

Personal data is any information that can be linked directly, or indirectly when combined with other data, to a living person. This means that widely differing data constitute personal data, e.g. name and contact details, as well as details and information about the suspected irregularity reported through the internal reporting channels.

It is important to Billerud that your personal data are processed responsibly and securely and in accordance with applicable laws, especially the General Data Protection Regulation (“GDPR”). This privacy notice describes how we process your personal data in connection with whistleblowing and what rights you have in connection with it.

We may process personal data about you if you:

- submit a report, i.e., if you are the “whistleblower”, and if you choose to not be anonymous;
- are the subject of a report, i.e. the person suspected of the alleged irregularity;
- are a potential witness of the alleged irregularity; and
- in other ways are affected by or connected to the alleged irregularity or relevant to the investigation of such irregularity.

2. WHAT PERSONAL DATA DO WE PROCESS ABOUT YOU?

The personal data processed within, or in connection to, the reporting system may include:

- information on who has submitted the report (if the person reporting chooses to provide such information), the individual suspected of the alleged irregularity, possible witnesses or individuals in other ways affected by or connected to the alleged irregularity or relevant to the investigation of such irregularity;
- contact information to the individuals listed above (e.g., name, position, e-mail and phone number);
- details on the alleged irregularity; and
- information relating to the follow up of the alleged irregularity.

We do not make automated decisions by processing your personal data (e.g., profiling you).

3. FOR WHAT PURPOSES DO WE PROCESS YOUR PERSONAL DATA?

We process the personal data listed above for the purposes listed below.

- The personal data collected through Speak-up Line or other information relating to the alleged irregularity is processed to administrate and investigate the allegations submitted to handle irregularities in accordance with what is set out in the Group Directive on whistleblowing.
- The information discovered in connection with reports submitted through Speak-up Line may also give rise to certain HR related implications, such as e.g., disciplinary actions. In such case, the personal data is processed for the purpose of carrying out such HR related implications.

4. WITH WHAT LEGAL BASIS DO WE PROCESS YOUR PERSONAL DATA?

4.1 Legal basis for processing in Speak-up Line

The legal basis for the processing of personal data is that the processing is necessary for compliance with applicable legal obligations with regards to whistleblowing.

Billerud also has a legitimate interest of identifying and duly dealing with irregularities or wrongdoings, to establish a safe and comfortable work environment and to report suspected offences to law enforcement authorities.

Special categories of personal data, such as data about health, or data relating to criminal convictions and offences, may be processed in Speak-Up Line. Billerud legal basis for such processing is that that the processing is necessary for the compliance with a legal obligation.

For Billerud “Rockhammar”, “Billerud Germany GmbH”, “Billerud France”, “Billerud Spain”, “Billerud Italy”, “Billerud Lithuania”, “Billerud Estonia” (legal entities within the EU with less than 50 employees), legal compliance requires that personal data about legal offences of wrongdoings may only be processed in reference to persons in key or leadership positions within Billerud¹.

4.2 Legal basis for processing of personal data in connection with potential HR related implications

The legal basis for the processing of personal data relating to potential HR related implications as described above is that it is necessary for the establishment, exercise or defence of legal claims. It may also, for some processing, be based on the legitimate interest of identifying and duly dealing with irregularities or wrongdoings.

¹ By persons in key or leadership positions, we mean all persons in leading positions at any entity within the Billerud group, Group Management Team, Board members and other key employees with a decision making role in the business at any entity within the Billerud group, or anyone else who is regarded at Billerud as a key employee.

5. HOW DO WE GAIN ACCESS TO YOUR PERSONAL DATA?

When you have not given us your personal data yourself, we could have received the personal data from another person e.g., the person who have submitted a report through Speak-up Line or in other ways given the personal data in connection with the investigation or follow-up of an alleged irregularity.

6. TO WHOM DO WE DISCLOSE YOUR PERSONAL DATA?

We may disclose personal data to law enforcement authorities, independent auditors or external advisors for the purposes required to duly handle any reported wrongdoings, such as conducting investigations or seeking legal advice. If you are a whistleblower, we will inform you prior to sharing any information that may reveal your identity, unless informing you would jeopardize the follow up on the report and the subsequent investigations.

Our IT suppliers and other partners who manage personal data on our behalf, so-called data processors, must always sign an agreement with us so that we can ensure a high level of protection of your personal data with them as well. Specific safeguards are implemented with regard to partners outside the EU/EEA, such as entering into agreements that include the standard model clauses for data transfer adopted by the EU Commission and which are available on the EU Commission's website.

The data processors that may need to access your personal data are e.g., external partners that perform tasks on our behalf, e.g., supply IT services or providing the whistleblowing system.

The whistleblowing software used by Billerud is provided by: WhistleB. WhistleB provides the technical infrastructure on which your personal data is stored, but it does not gain any access to your personal data.

If we share your personal data with a recipient who is an independent data controller for their processing of your personal data, the recipient is responsible for the lawfulness of the processing in question.

The following recipients/categories of recipients may receive data of yours:

- Public authorities that need to be involved in investigations; and/or
- Law firms and external consultants that need to be involved in investigations.

7. SECURITY FOR THE PROTECTION OF PERSONAL DATA

We safeguard your personal data with a high level of security and to this end we have implemented appropriate technical and organisational security measures to protect your personal data from unauthorised access, change, dissemination or destruction.

For instance, the handling of the personal data is restricted to competent persons who handle reports and investigate suspected irregularities. All information in reports made through, or other information relating to, Speak-up Line will be treated as confidential and sensitive.

The identity of the individual that submitted the report is protected by confidentiality, meaning that no information provided by such individual may under any circumstances be disclosed. Where it is necessary for the follow up on the report and the subsequent investigations, information that may reveal the identity of the whistleblower and other individuals involved in the matter may be shared only with those who strictly need the information for such follow up and investigation.

8. WHEN IS YOUR PERSONAL DATA ERASED?

Personal data that is obviously irrelevant to the processing of a particular whistleblowing report will not be processed by us. If such personal data have been collected by mistake, it will be deleted without undue delay.

The personal data that is processed in connection with Speak-up Line will be erased without undue delay when the personal data is no longer necessary in relation to the purpose, e.g., when it has been finally concluded that a reported person is no longer a suspect for any irregularity.

If it is concluded that a sanctionable behaviour of the reported person is given and appropriate measures have been taken against such person, the personal data of the whistleblower and any witnesses will be anonymized. The personal data of the reported person will be stored in his/her personal file.

Should applicable legal obligations require longer storage periods, we will store the personal data of all people involved according to these legal obligations.

If we have disclosed personal data to law enforcement authorities or other third parties processing the personal data in capacity of controller, such third parties may process the personal data also after our erasure.

9. YOUR RIGHTS

You have certain rights in relation to us. These are set out in general below.

- **Right of access** (register transcript) – a right to information about our processing of your personal data and access to it.

When the personal data have been collected, the person or persons concerned by a report in the whistleblowing system will also receive specific information thereon according to the Speak-Up Line Directive, as long as it would not jeopardize the investigation of the matter.

Information must also be provided to anyone who makes a request for information as to whether there is personal data registered about him/her. Information, or the reason for not disclosing requested information, shall as a main rule be provided without undue delay and within one month after the date on which the request was made. However, the information must not disclose the identity of the person who submitted the report.

- **Right to rectification** – a right to have erroneous data rectified and add such personal data that is missing.
- **Right to object** – a right to object to our personal data processing about you if it takes place based on a legitimate interest.
- **Right to erasure** – a right to have your personal data erased under certain circumstances unless the data is necessary for a particular purpose or there is another legal ground for the processing.
- **Right to limitation of processing** – a right to request that personal data processing is restricted, e.g., if you contest the accuracy of the data. Our access to the data is restricted while the accuracy of the data is investigated.
- **Right to data portability** – a right to request that personal data are transferred from one data controller to another. This right is restricted to personal data that you have supplied to us yourself.

Any request to exercise your rights shall be sent via the Speak-Up Line to the Speak Up Line Officer. You also always have the right to file a complaint to the Swedish Authority for Privacy Protection (IMY) (www.imy.se) if you think that your personal data is being processed in violation of applicable legislation.
