Version: 2
Date of last update: 10-06-2025

WHISTLEBLOWING PRIVACY POLICY
INFORMATION REGARDING PROCESSING OF PERSONAL DATA

WE CARE ABOUT YOUR PRIVACY

Your trust is important to us. Our aim is that you feel safe when you share your personal data with us. Personal data is any information that can be used to identify an individual.

We take appropriate measures to ensure that your personal data is always safe with us. These measures include, for example, the control of physical access to the premises where the data processing is carried out, the training of the persons involved in the processing of personal data, the continuous and periodic security risk assessment, the management of access rights and technological security, such as the use of encryption, secure data transmission, etc. We take appropriate measures to ensure that the processing of your personal data complies with applicable data protection laws, our internal policies, guidelines and procedures. We have also assigned a Data protection officer whose task is to monitor that we follow these laws, guidelines and routines.

It is important for us to be transparent with how we handle your personal data. In this information text, we therefore describe how and where we process personal data in the context of Whistleblower Process in Rimi and protecting Whistleblower from retaliation.

WHICH CATEGORIES OF PERSONAL DATA DO WE COLLECT AND WHY?

- **Management of Whistleblowing Process.**

We process your personal data by receiving, examining and investigating Whistleblowing reports. In order to be able to receive and analyse the reports, make decisions about them, we carry out the following processing of personal data.

- Receiving Whistleblowing reports.
- First screening whether the report is appropriate/ inappropriate as Whistleblower Case.
- Collection of information necessary for the investigation.
- Carry out investigation regarding information provided in the report and collected during the investigation and make a decision concerning the report.

Categories of personal data	• **Identity information** *(name, surname, personal code, etc.)* • **Demographic data** *(date of birth, if indicated instead of personal code, etc.)* • **Company information** *(name of the company, person's job title, etc.).* • **Employment information** *(time and date of employment, type of employment, position, job duties, workplace, etc.).* • **Internship data** *(the time of the internship – if the reporter or the person concerned is /was a intern, etc.).* • **Contact details** *(e. g. personal phone number, personal e-mail, home address).* • **Communication data** *(e.g., metadata, content of e-mail, phone call, etc.).* • **Information about situation** *(e.g., type of situation, time and date when situation occurred, description of situation, accompanying documents, etc.).* • **User generated personal data** *(e.g., information about activities within our information systems, behavior in digital channels, confirmation of the reporter that he/she is aware of legal consequences of providing false information and confirmation*

	that the provided information is correct; Whistleblower's choice to provide the report based on the Law of Protection of Whistleblowers or not, etc.). • **Audio-visual material** *(e.g. audio recording - if the meeting with the Whistleblower is recorded, photos, CCTV record, etc.).* • **For fulfillment of legal obligation** • **Other data that are provided and/or necessary during the investigation of the report.**
Legal basis	To fulfil our legal obligation
Retention period	• If the Whistleblower submitted a report in accordance with the Law on protection of Whistleblowers, personal data are stored for 5 years from the date of the last decision to investigate the information was provided. • If the Whistleblower provided the report but did not provide it under the Law on protection of Whistleblowers (e.g. report was anonymous, etc.), personal data are deleted within 2 months from the end of the investigation, unless they are needed to establish, exercise or defend legal claim. • If the report is not deemed as „Whistleblower Case" and it is not investigated on company's initiative, personal data are deleted after 30 days after the decision not to investigate is adopted. • When data are processed to establish, exercise or defend legal claim: – and the case is heard in a court, the data shall be store for 1 year after the final an non-appealable decision is adopted. – and the case is not heard in court, but the claim was not resolved, data are stored until the claim is resolved, but not longer than the person can defend his/her violated rights in accordance with statutory limitation periods.

- **Management of communication with the applicant or Whistleblower.**

We process your personal data in order to contact you and communicate with you regarding your application or report through Whistleblowing channel. For this purpose we carry out the following data processing:

- Execution of communication with you, when you have written to us (e.g. when you contact us for consultation regarding Whistleblowing Process.)
- Maintaining contact with the Whistleblower by the communication method chosen by Whistleblower when clarification is needed about the details of the report or inform the Whistleblower about actions taken regarding the report.

Categories of personal data	• **Identity information** *(name, surname, personal code, etc.)* • **Contact details** *(e. g. personal phone number, personal e-mail, home address).* • **Communication data** *(e.g., metadata, content of e-mail, phone call, etc.).* • **For fulfillment of legal obligation.**
Legal basis	To fulfil our legal obligation
Retention period	• If Whistleblower provided the report in accordance with the Law on protection of Whistleblowers, personal data is stored for 5 years from the date of the last decision to investigate the information was adopted. • If Whistleblower provided the report but did not submit it according to the Law on protection of Whistleblowers (e.g. the report was anonymous, etc), personal data shall be deleted after 2 months after the end of investigation, except when data are processed to establish, exercise or defend legal claim. • If the report is not deemed as „Whistleblower Case" and it is not investigated on company's initiative, personal data are deleted after 30 days after the decision not to investigate is adopted. • When data are processed to establish, exercise or defend legal claim:

	– and the case is heard in a court, the data shall be store for 1 year after the final an non-appealable decision is adopted. – and the case is not heard in court, but the claim was not resolved, data are stored until the claim is resolved, but not longer than the person can defend his/her violated rights in accordance with statutory limitation periods.

- **Reporting to the authority about the received Whistleblower's report.**

If you choose to report anonymously, we will not try to identify you and will not provide your data to the authority, unless we are obliged to do so.
If the report was not anonymous, we process your personal data in order to report to national authority, when required by local Law on the Protection of Whistleblowers, that Whistleblower's report was received. Authority must be informed, when:

- Whistleblower submitted the report on the Law on the Protection of Whistleblowers and asked for Whistleblower's protection granted by authority.
- In case alleged illegal activities indicated in Law on the Protection of Whistleblowers were or planned to be committed.

For this purpose we process the following data.

Categories of personal data	• **Identity information** *(name, surname, personal code, etc.)* • **Demographic data** *(date of birth, if indicated instead of personal code, etc.)* • **Contact details** *(e. g. personal phone number, personal e-mail, home address).* • **Information about situation** *(e.g., type of situation, time and date when situation occurred, description of situation, accompanying documents, etc.).* • **For fulfillment of legal obligation.**
Legal basis	To fulfil our legal obligation
Retention period	• If Whistleblower provided the report in accordance with the Law on protection of Whistleblowers, personal data is stored for 5 years from the date of the last decision to investigate the information was adopted. • If Whistleblower provided the report but did not submit it according to the Law on protection of Whistleblowers (e.g. the report was anonymous, etc), personal data shall be deleted after 2 months after the end of investigation, except when data are processed to establish, exercise or defend legal claim. • If the report is not deemed as „Whistleblower Case" and it is not investigated on company's initiative, personal data are deleted after 30 days after the decision not to investigate is adopted. • When data are processed to establish, exercise or defend legal claim: – and the case is heard in a court, the data shall be store for 1 year after the final an non-appealable decision is adopted. – and the case is not heard in court, but the claim was not resolved, data are stored until the claim is resolved, but not longer than the person can defend his/her violated rights in accordance with statutory limitation periods.

- **Protecting Whistleblower from retaliation.**

Whistleblower's identity is kept confidential during all the stages of Whistleblower process and after it ends, except when there is a need to fulfil legal obligation to ensure protection from retaliation. In this case information about the Whistleblower, or his relative or supporter may be disclosed the to their manager or to other person who is making decision to ensure their protection from retaliation (e. g. worsening of employment conditions, termination, etc.).
For this purpose we process the following data.

Categories of personal data	• **Identity information** *(name, surname, personal code, etc.)* • **Company information** *(name of the company, person's job title, etc.).* • **Employment information** *(time and date of employment, type of employment, position, job duties, workplace, etc.).* • **Internship data** *(the time of the internship – if the reporter or the person concerned is /was a intern, etc.).* • **For fulfillment of legal obligation.**
Legal basis	To fulfil our legal obligation
Retention period	• If Whistleblower provided the report in accordance with the Law on protection of Whistleblowers, personal data is stored for 5 years from the date of the last decision to investigate the information was adopted. • If Whistleblower provided the report but did not submit it according to the Law on protection of Whistleblowers (e.g. the report was anonymous, etc), personal data shall be deleted after 2 months after the end of investigation, except when data are processed to establish, exercise or defend legal claim. • If the report is not deemed as „Whistleblower Case" and it is not investigated on company's initiative, personal data are deleted after 30 days after the decision not to investigate is adopted. • When data are processed to establish, exercise or defend legal claim: – and the case is heard in a court, the data shall be store for 1 year after the final an non-appealable decision is adopted. – and the case is not heard in court, but the claim was not resolved, data are stored until the claim is resolved, but not longer than the person can defend his/her violated rights in accordance with statutory limitation periods.

- **Management of legal claims.**

We process your personal data in order to establish, exercise and defend legal claim and to protect company's interests.

Categories of personal data	All the data categories mentioned above: • **Identity information** *(name, surname, personal code, etc.)* • **Demographic data** *(date of birth, if indicated instead of personal code, etc.)* • **Company information** *(name of the company, person's job title, etc.).* • **Employment information** *(time and date of employment, type of employment, position, job duties, workplace, etc.).* • **Internship data** *(the time of the internship – if the reporter or the person concerned is /was a intern, etc.).* • **Contact details** *(e. g. personal phone number, personal e-mail, home address).* • **Communication data** *(e.g., metadata, content of e-mail, phone call, etc.).* • **Information about situation** *(e.g., type of situation, time and date when situation occurred, description of situation, accompanying documents, etc.).* • **User generated personal data** *(e.g., information about activities within our information systems, behavior in digital channels, confirmation of the reporter that he/she is aware of legal consequences of providing false information and confirmation that the provided information is correct; Whistleblower's choice to provide the report based on the Law of Protection of Whistleblowers or not, etc.).* • **Audio-visual material** *(e.g. audio recording - if the meeting with the Whistleblower is recorded, photos, CCTV record, etc.).*

	• **For fulfillment of legal obligation.** • **Other data that are provided and/or necessary during the investigation of the report.**
Legal basis	Our legitimate interest
Retention period	• If Whistleblower provided the report in accordance with the Law on protection of Whistleblowers, personal data is stored for 5 years from the date of the last decision to investigate the information was adopted. • If Whistleblower provided the report but did not submit it according to the Law on protection of Whistleblowers (e.g. the report was anonymous, etc), personal data shall be deleted after 2 months after the end of investigation, except when data are processed to establish, exercise or defend legal claim. • If the report is not deemed as „Whistleblower Case" and it is not investigated on company's initiative, personal data are deleted after 30 days after the decision not to investigate is adopted. • When data are processed to establish, exercise or defend legal claim: – and the case is heard in a court, the data shall be store for 1 year after the final an non-appealable decision is adopted. – and the case is not heard in court, but the claim was not resolved, data are stored until the claim is resolved, but not longer than the person can defend his/her violated rights in accordance with statutory limitation periods.

FROM WHICH SOURCES DO WE COLLECT PERSONAL DATA?

- **Yourself**

Personal data are collected from the applicant and Whistleblower from the communication means, from the report, added documents, additionally provided information.

- **Third persons**

During the investigation information may be collected from other persons – Business partners, witnesses, people concerned, other people who might provide information necessary for the investigation.

- **Information systems**

During preliminary evaluation of the report and during investigation data may be processed from our own information systems.

SHARING OF PERSONAL DATA

- **Service providers**

We might share your personal data with companies that provide services to us, such as:

- Data hosting services;
- Information system development and maintenance services;
- External lawyers.

These service providers can only process your personal data according to our instructions and not use them for other purposes. They are also required by law and our cooperation agreement to protect your personal data.

- **External consultants and insurance companies**

If it is necessary to protect interests of our company we may transfer your personal data to insurance companies or external consultants, such as auditors, lawyers or other independent advisors, who act as independent data controllers and whose activities are regulated by law.

- **Group companies**

We do not share personal data received through local internal Whistleblower channel with Rimi group companies, except when there is a need to involve investigator with specific expertise to solve the issue from different Rimi group company. In this case an involved investigator obliges to keep information from Whistleblower Case confidential.

- **Law enforcement authorities, state and local government institutions**

To fulfil our legal obligation we may transfer your personal data to law enforcement authorities.
We may also transfer your personal data to law enforcement authorities, state and local government institutions in order to establish, claim and defend legal claims.

WHERE DO WE PROCESS YOUR PERSONAL DATA?

We always aim to process your personal data within EU/EEA.
In certain cases, we may transfer or process your personal data outside the territory of EU/EEA. For example, for IT or other support we may use service providers who access personal data from the countries outside EU/EEA. We may use service providers that are located in various countries outside EU/EEA, when data transfer depends on the time of the day (principle „follow-the sun“).
When your data is processed by our service provider outside EU/EEA, we always ensure that adequate technical and organisational measures are in place to ensure that recipients process data securely.
When we transfer your personal data to a country outside EU/EEA, we use Standard contractual clauses or an Adequacy decision as a transfer mechanism. In rare cases, our service provider, which acts as a data processor, may transfer personal data to a sub-processor outside EU/EEA applying Binding corporate rules of the company as transfer mechanism. Countries for which adequacy decisions were adopted can be found here. Standard contractual clauses of the EU can be found here.
You can request that we provide you the information, in which countries your personal data is processed. In such cases, please submit us a written request.

FOR HOW LONG ARE YOUR PERSONAL DATA STORED?

When the retention period is specified by national or international laws, we will comply with the requirements of the legislation for the retention period.
When the Whistleblower submitted his report in accordance with the Law on the Protection of Whistleblowers and required protection of the Whistleblower by this Law, personal data shall be processed for 5 years from the last decision to examine the provided information, unless it is necessary to process the data longer.
When the Whistleblower used Whistleblower service, but did not submit his report in accordance with the Law on the Protection of Whistleblowers, personal data in a Whistleblower Case shall be deleted within 2 months of the conclusion of the investigation, unless data are processed to establish, enforce or defend legal claims.
When case is not considered as Whistleblower Case and is not investigated by company's initiative, it can be dropped. Then personal data shall be deleted within 30 days upon decision to drop the case.
When data are processed to establish, exersice or defend legal claim:

- If the court case is ongoing, then data are processed for 1 year after the final not appealable decision of the court was adopted.
- If there is no court case but the claim was not resolved – then data are processed till the claim is solved, but not longer than a person can defend his violated right according to the terms set in law by bringing a claim to the court.

YOUR RIGHTS

Data protection laws give you a number of rights with regards to the processing of your personal data.

- **Access to personal data**

You are entitled to request confirmation from us if we process personal data relating to you, and in such cases request access to the personal data we are processing about you. To carry out the mentioned right, please, provide a written request to our Whistleblower Team.

- **Rectification of personal data**

Furthermore, if you believe that information about you is incorrect or incomplete, you have the right to correct it yourself or ask us to do it. To carry out the mentioned right, please, provide a written request to our Whistleblower Team.

- **Objection against processing based on a legitimate interests**

You are entitled to object to personal data processing based on our legitimate interests. However, we will continue to process your data, even if you have objected to it, if we have compelling motivated reasons for continuing to process data, for example for establishing, enforcing or defending legal claim.
To carry out the mentioned right, please, provide a written request to our Whistleblower Team or to our Data protection officer.

- **Erasure**

Under certain circumstances, you have rights to ask us to delete your personal data. However, this does not apply if we are required by law to keep the data or personal data are needed for us to establish, exercise or defend legal claim. To carry out the mentioned right, please, provide a written request to our Whistleblower Team or to our Data protection officer.

- **Restriction of processing**

Under certain circumstances, you are also entitled to restrict the processing of your personal data. To carry out the mentioned right, please, provide a written request to our Whistleblower Team or to our Data protection officer.

WHOM CAN YOU CONTACT IF YOU HAVE ANY QUESTIONS?

If you have any questions about the processing of your personal data, please feel free to contact us.
If you are not satisfied with the response you received, you are entitled to file a complaint with the Data Inspectorate in Latvia – https://www.dvi.gov.lv/.

- **Contact details of company in charge of handling your personal data**

SIA Rimi Baltic, reg. No. 40003592957,
Legal address: 161 A. Deglava iela, Riga, Latvia, LV 1021
Phone number: +371 67045409
Email: info.lv@rimibaltic.com,

- **Whistleblower Team contact details:**

In order to ensure confidentiality, you can consult about data processing with Whistleblower Team by email: report.lv@rimibaltic.com.

- **Contact details of the Data Protection Officer**

Email: RimiDPO@rimibaltic.com
You also can contact our Data protection Officer by sending a letter to us at the above mentioned address and addressing it to the Data protection officer.

CHANGES AND UPDATES TO THIS PRIVACY POLICY

We may update this Privacy policy, for example if new purpose for the processing of personal data is added or new legal requirements are introduced. The latest version of this Privacy policy is available in our website.