

Version: 03

Date of last update: 09.10.2020.

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 always is safe with us and that the processing of your personal data is compliant with present data protection laws, our internal policies, guidelines and routines. 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 **visitor registration and access management**.

WHICH CATEGORIES OF PERSONAL DATA DO WE COLLECT AND WHY

The main purpose throughout all access management activities is to deny physical access of any unauthorized person inside restricted areas and to protect our property, assets and our employees.

- **To ensure secure access management to our office, store back office and DC's**

We process your personal data in order to control access to our office, stores back-office and DCs, e.g., to register you as a visitor, to keep track who entered and left our premises, to notify the recipient that you have arrived, to keep you updates about waiting time.

We reserve the right to ask you to show to our security guard or secretary identification document to check your identity.

These premises can be visited only by authorized personnel therefore you should register yourself and/or your company should provide to us information about who you are, who you are visiting, how many persons from which company will be arriving. Upon your arrival we might ask you to indicate your time of arrival and departure and what company you represent.

Categories of personal data	Legal basis	Retention period
<ul style="list-style-type: none">• Identity information, e.g., name, surname, username, customer ID etc.• Company information, e.g., name of the company, person's job title etc.• Contact details, e.g., email, phone number, address etc.• Information about situation, e.g., type of situation, time and date when situation occurred, description of situation, accompanying documents etc.• Authentication information, e.g., information on electronic signature, a password, a secret question, a verification code etc.	Our legitimate interests	No longer than 1 year after data are entered in visitor registration system or journal.

- **To ensure use of our parking lot**

In some specific cases we may process your personal data in order to provide you possibility to use our parking lot free of charge, e.g., to register in our documents and systems that car with your provided car registration number can use our parking lot for agreed purposes and time.

Categories of personal data	Legal basis	Retention period
<ul style="list-style-type: none"> • Identity information, e.g., name, surname, username, customer ID etc. 	Our legitimate interests	Visitors up to 90 days, employees until they work in company and use parking lot

- **To ensure proper access key management process**

We process your personal data in order to control access to our restricted areas, e.g., to issue to you key (physical and electronic key) and keep track on your movement in our property.

Categories of personal data	Legal basis	Retention period
<ul style="list-style-type: none"> • Identity information, e.g., name, surname, username, customer ID etc. • Information about situation, e.g., type of situation, time and date when situation occurred, description of situation, accompanying documents etc. • Authentication information, e.g., information on electronic signature, a password, a secret question, a verification code etc. • User generated personal data, e.g., information about activities within our information systems, behavior in digital channels, saved shopping list, favorite store etc. 	Our legitimate interests	As long as key is issued to you.

- **Fraud prevention and management of legal claims**

We may process your personal data to defend, establish and exercise legal claims, including to prevent and /or stop fraudulent or criminal activity, gather evidence concerning detected issues and manage the situation.

Categories of personal data	Legal basis	Retention period
<ul style="list-style-type: none"> • Identity information, e.g., name, surname, username, customer ID etc. • Company information, e.g., name of the company, person's job title etc • User generated personal data, e.g., information about activities within our information systems, behavior in digital channels, saved shopping list, favorite store etc. • Information about situation, e.g., type of situation, time and date when situation occurred, description of situation, accompanying documents etc. • Any other specific information, which is relevant for particular investigation and legal claim 	Our legitimate interest	While investigation, settlement and implementation of legal claim takes place. If violation is not discovered within investigation, data will be retained for 1 (one) year after the decision to close investigation. If violation discovered, data will be retained for 3 (three) years after the decision to close investigation or until final implementation of court decision.

- **Management of access to wireless network during your visit**

We process your personal data to grant access to our provided wireless network while you visit our premises and to protect our legitime interest in case you have violated wireless network terms of use.

Categories of personal data	Legal basis	Retention period
<ul style="list-style-type: none"> • Identity information, e.g., name, surname, username, customer ID etc. • Contact details, e.g., email, phone number, address etc. • Connection data, e.g., device type, operation systems and version, time zone, type of browser etc • User generated personal data, e.g., information about activities within our information systems, behavior in digital channels, saved shopping list, favorite store etc. 	Our legitimate interest	30 calendar days after you requested access to wireless network

FROM WHICH SOURCES DO WE COLLECT PERSONAL DATA?

- **Yourself**

We collect the personal data you provide to us directly, for example, when you visit our premises, provide information, and indirectly, for example, by using our wireless network.

- **Our service providers**

We collect the personal data from your company what you represent, for example, when they provided to us information who will visit us.

- **Other sources**

We collect personal data from used technical systems, for example, audit logs of use of issued electronic key from access management systems.

SHARING OF PERSONAL DATA

- **Service providers**

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

- data hosting services
- information system development and maintenance services
- physical security services

These companies 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.

- **Group companies**

We may share your personal data with relevant Rimi Baltic group companies if it is necessary for achieving defined purposes.

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

To fulfill our legal obligation we may transfer your personal data to law enforcement authorities, state and local government institutions upon their request. We may also transfer your personal data to law enforcement authorities, state and local government institutions in order to meet our legitimate interest in establishing, claiming and defending legal claims.

- **Other companies**

For the purposes mentioned in this information text we may share your Identity information and/or Company information with other companies who act as separate data controllers. We share such information to ensure that you can access respective premises what are under other company access control, use their parking lot or receive needed keys.

WHERE DO WE PROCESS YOUR PERSONAL DATA?

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

Your personal data is not transferred or processed in a country outside EU/EEA.

FOR HOW LONG ARE MY PERSONAL DATA STORED?

Personal data recorded in access management and visitor registration systems and journals will be retained no longer than 1 year.

Personal data recorded in paper or in other form regarding register of issuance and return of keys or using parking lot will be retained for the whole periods the key or parking lot is issued to the person.

Personal data in relation with access to wireless network and use of it will be retained for 30 calendar days after you requested access to wireless network.

If data are needed for fraud prevention and management of legal claim data will be retained while investigation, settlement and implementation of legal claim takes place. If violation is not discovered within investigation, data will be retained for 1 (one) year after the decision to close investigation. If violation discovered, data will

be retained for 3 (three) years after the decision to close investigation or until final implementation of court decision.

YOUR RIGHTS

Data protection laws give you a number of rights with regards to the processing of your personal data. Please be informed that we do not have aim to identify you if it is not necessary for achieving defined purposes.

- **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 us or to our Data protection officer.

- **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 us or to our Data protection officer.

- **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. To carry out the mentioned right, please, provide a written request to us 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. To carry out the mentioned right, please, provide a written request to us 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 us or to our Data protection officer.

WHO DO I CONTACT IF I 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.

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

Rimi Eesti Food AS, reg. No. 10263574,
Legal address: Põrguvälja tee 3, Pildiküla, Rae vald, Harjumaa
Phone number: +372 605 9400
Email: info.ee@rimibaltic.com,

- **Contact details of Customer service**

Phone number: +372 605 6333

Email: klienditugi.ee@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.