Annex 9-1 – MOBILE APP PIRNAR PRIVACY POLICY

1. Preliminary provisions

At PIRNAR d.o.o., we are committed to ensuring the highest standards of data protection and privacy. For this purpose, we provide you with documents where you can learn about your rights, obtain information about how we use your personal data and how we process it.

Personal data means any information that directly or indirectly relates to an identified or identifiable individual. The EU General Data Protection Regulation (GDPR) constitutes the legal basis for data protection.

2. Overview

The data processing carried out by PIRNAR in the context of the use of our entrance doors and the Pirnar application (hereinafter referred to as the application) can mainly be divided into five categories:
• when downloading our application, the necessary information is provided to the respective online store from which you download the application.
• to use the application and later connect to the PIRNAR entrance door with the built-in SecuroSmart system and manage it, registration in the application is required. When registering, certain information is requested from the user.
• in order to provide many features, such as the option to give easy feedback, our application needs access to various features and sensors of your mobile device.
• when using our application, different data is exchanged between your end device on which you use the application and our server on the other side. Exchanged information may include personal data. We use the information collected in this way for, inter alia, the following purposes:
• to facilitate your use of the PIRNAR entrance door with the built-in SecuroSmart system and its functions,
• to optimize our application and the PIRNAR entrance door with the built-in SecuroSmart system
• to display ads in the browser of your end device from which you access the application or through so-called push notifications.

3. Downloading the application

When downloading our application, the online store manager in question (Apple App Store or Google Play) automatically processes mainly the following data:
• the user name in the online store,
• the e-mail address stored in the online store,
• the account number in the online store,
• the time and date of the transfer,
• payment details; and

• the individual device identification number.
PIRNAR has no influence over this data collection and is not responsible for it. More information about this data processing can be found in the data protection provisions of individual online store managers:
• Google Play Store: https://policies.google.com/privacy?hl=en-US
• Apple App Store: https://www.apple.com/legal/privacy/en-ww/

4. Registering in the application

Purposes of data processing/legal bases
In order to use the features in the application, you must first register and create an account.
At the time of registration, the following information shall be collected in any case:
• e-mail address or (if your version offers this option) user name and login name
• user ID assigned to you by us
• country ID
• your password, set up in accordance with the technical requirements (stored in encrypted form)
In addition, the following information shall be stored at the time of registration:
• IP address of the user,
• time zone of the user,
• date and time of registration.

We process your login data in order to identify your login and comply with the requirements for resetting your password. We process other information that you provide to us as part of your registration or login in order to (1) verify your eligibility to manage your account, (2) enforce the terms of use of the application and any associated rights and obligations, and (3) contact you so that we can, for example, provide you with any technical or legal instructions, updates, safety-related messages or other communications relating to the management of your account.

If you have provided personal data in our application at the time of registration, we process this data on the basis of Article 6(1)(b) of the GDPR, as this data is necessary for the performance of the contract for the use of the Pirnar application.

Data retention period/criteria for determining the data retention period
Registration information is retained until you deactivate or delete the Pirnar application or otherwise let us know that you no longer wish to use the Pirnar application and the associated user account.

5. Using the application

Purposes of data processing/legal bases
When using our Pirnar application, we automatically and without need for any action on your part transfer to our servers
• the IP address of your mobile device,
• the country code of your mobile device,

• the date and time of access,
• the customer's request and its content,
• the HTTP response code; and
• the amount of data transferred
and temporarily store them in a so-called log file for the following purposes:
• protection of our systems,
• error analysis,
• prevention of abuse or fraud.

The legal basis for the processing of an IP address is Article 6(1)(f) of the GDPR. Our legitimate interest stems from the aforementioned purposes of data processing.

Data retention period/criteria for determining the data retention period
The data is stored for a period of 14 days and then automatically deleted, unless you have given explicit consent for the data to be used for a longer period.

6. Connecting the application Pirnar to the PIRNAR entrance door with the SECUROSMART system

When you connect our Pirnar application to the PIRNAR entrance door with SecuroSmart on, further personal data is collected.
Your profile information
After registering in the application, you voluntarily create different profiles, including your user profile, your home, other users of the device and groups. This information is stored in the application for later use, as it is necessary for the use and management of the PIRNAR entrance door with the built-in SecuroSmart system and is therefore processed during use if necessary:
• under personal settings, you can choose a nickname, upload an image of your choice (which will appear as the user's avatar), select a time zone and provide your contact information (to receive notifications, for example).
• in order to assign a PIRNAR entrance door with a built-in SecuroSmart system, you must specify one or several homes (My Home) in the Home Management section. For this purpose, we process the selected name of your home (My Home) where you intend to use the PIRNAR entrance door with the built-in SecuroSmart system, the location tag (Home Location), the ID tag that was assigned by us (Home-ID) and the list of the SecuroSmart system.
• you can also enable other users to use your PIRNAR entrance door with the SecuroSmart built-in system and define the scope of authorisations (administrator, common member), for which the user names of additional users (which they receive when registering the application), their user IDs, input codes and, if necessary, the selected user names are processed. If the input functions enable user-specific settings, further input user data such as contact information are also processed.
This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.
You can manage your profile information in our application and delete it if necessary. We will keep your data until you delete it in our application. If you disconnect your PIRNAR entrance door with the

SecuroSmart built-in system in your application and select remove device or remove device and wipe data, your data relating to this input will be deleted as soon as you disconnect the device from the application.

Your usage data

Through our Pirnar application, we then process further personal data according to what is necessary to ensure certain functions and compliance with selected individual settings. This may concern in particular the following categories of data:

Category of data	**Examples**	**Possible purposes and justification**
Input identification data	PPR work order	Identifying the product and enabling login in the network and in the application. This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.
Settings data	Default system settings or user-selected settings, in particular scenes, measures, automatic procedures or user-selected conditions (name, ID, background, conditions, sequences and activities will generally be stored).	This data is necessary to provide the necessary functions, if available, that the user has chosen. This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.
Usage data	Information on when and how you use services that include typical log data, system data (system type, system properties, system status and updates), user actions or choices during the use of the system (selected time zone), information on energy consumption, etc. This data may allow conclusions to be drawn as to the behaviour and location of	This data is necessary to provide the necessary functions. This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.

	the user in the premises in which the system is used.	
Substantive data	Information that the system generates from you according to its mode of operation that enable the drawing of conclusions about your behaviour.	This data is necessary to provide the necessary functionality (this is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request).
Sensor data	Information recognised, recorded or transmitted by sensors in the system, such as sound recordings and images, wind speed, moisture sensors (in the case of video recordings, for examples).	This data is necessary to provide the necessary functions. This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.
Contact data	e-mail address, user name	

Specific categories of personal data are not intended to be collected and processed (i.e. data on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data allowing direct identification of a natural person, health data, data on sexual life or sexual orientation). We cannot guarantee, however, that sensors such as cameras and the like do not process this data or that findings regarding user behaviour cannot be made indirectly on the basis of the usage data. We will not process such data for our own purposes or perform such analyses.

When connecting and setting up the PIRNAR entrance door with the built-in SecuroSmart system supported by the Pirnar application, you will always be specifically informed about the features available and, if necessary, also about the data processed in each case to carry out the respective functions. We will notify you of significant changes, such as the scope of the offer or technically necessary changes, to the e-mail address you provided at the time of registration and/or through our Pirnar application.

You can manage the data of your PIRNAR entrance door with the built-in SecuroSmart system in our Pirnar application and delete it if you want. We will keep your data until you delete it in our Pirnar application. In your Pirnar application, if you disconnect from an individual SecuroSmart system, your data relating to that device will be deleted as soon as you disconnect the PIRNAR entrance door with the built-in SecuroSmart system from the Pirnar application.

Voice control via Google Assistant, Apple Siri, Amazon Alexa
You have the option to use certain functions (brightness and colour of LED lights, unlocking) of your PIRNAR entrance door with the built-in SecuroSmart system using the Google Assistant, Amazon Alexa or Apple Siri systems with voice commands. To use this management mode you need to connect the device to your Google Assistant, Apple Siri or Alexa.

If you operate your entrance door with the built-in SecuroSmart system via Google Assistant, Google LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043 (hereinafter referred to as Google) must provide personal information to your PIRNAR entrance door with the built-in SecuroSmart system or obtain personal information from your SecuroSmart system, exchanging the information necessary for the operation of the SecuroSmart system.

If you operate your entrance door with the built-in SecuroSmart system via Apple Siri,
Apple 1 Apple Park Way Cupertino, California, 95014-0642 (hereinafter referred to as Apple) must provide personal data to your PIRNAR entrance door with the built-in SecuroSmart system or obtain personal data from your SecuroSmart system, exchanging the information necessary for the operation of the SecuroSmart system.

If you operate your entrance door with the built-in SecuroSmart via Amazon Alexa, Amazon Corporate Headquarters Address: 410 Terry Ave. North, Seattle, WA, 98109-5210 (hereinafter referred to as Amazon) must provide personal data to your PIRNAR entrance door with the built-in SecuroSmart system or obtain personal data from your SecuroSmart system, exchanging the information necessary for the operation of the SecuroSmart system.

You can give voice commands to Google Assistant, Apple Siri or Amazon Alexa to operate your PIRNAR entrance door with the built-in SecuroSmart system or retrieve information from your SecuroSmart system. In doing so, data (in particular, data from your SecuroSmart system and speech data) is transferred to our servers and processed, while the necessary data is transferred to Google, Amazon or Apple who then use it to carry out the service. This data may include personal data. When you connect your Google Assistant, Apple Siri or Amazon Alexa account to the Pirnar application and activate Google Actions or Alexa in the Pirnar user menu, you expressly consent and authorise us to operate your entrance door with the built-in SecuroSmart system via Google Assistant, Apple Siri or Amazon Alexa and to transfer data through this system. The related processing of data by Google, Apple or Amazon is your own responsibility or the responsibility of Google, Apple or Amazon.

For information on how Google handles data, please refer to the Google Data Protection Statement, which is available at the following link:
https://support.google.com/googlenest/topic/7173611?hl=en&ref_topic=9371069,7029808,
and https://policies.google.com/privacy?hl=en-US We have no influence on how Google processes data.

For information on how Amazon Alexa handles data, please refer to Amazon Alexa's Data Protection Statement, which is available at the following link: https://www.alexa.com/help/privacy

We have no influence on how Amazon processes data.
We process your personal data on the basis of your consent (Article 6, paragraph 1, page 1, item a of the GDPR) as well as on the legal basis for the performance of the contract for the use of our Pirnar application, including voice control devices (Article 6, paragraph 1, page 1, item b of the GDPR), and exclusively for the purpose of handling your requests.

7. Access to your mobile device's features and sensors

Purposes of data processing/legal bases

- Location data

Our Pirnar application allows you to manage your devices partly with features that are tailored to the respective location of your end device. In order to provide you with specific services related to your location, you must consent to the collection of location data (under location settings, for example) in our Pirnar application or in your mobile device settings. There you can choose if your location monitoring function for the application should always be activated, only when using the application or only in individual cases. If you want to use this feature of the application, but have not given your consent to the collection of location data, a pop-up window will appear so that you can change your settings accordingly if necessary. You can change or deactivate this feature at any time in your mobile phone's operating system settings. The legal basis for the processing of your location data is your consent in accordance with Article 6(1)(a) of the GDPR.

- Photos/media/files on your mobile device/USB storage content (reading, editing, deleting)

If you use our Pirnar application to create content, such as photos and videos, via input devices, this content is stored directly on the memory of your mobile device or connected medium, depending on the location of installation of the application and the available memory.
This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.

- Microphones

The functions of the PIRNAR entrance door with the built-in SecuroSmart system can be partially controlled using the microphone of your mobile phone (for example: brightness and colour of LED lights, unlocking). In order to use features of this type, you must first grant Pirnar application access to your microphone in the operating system settings of your mobile phone. When you want to use this feature for the first time, the Pirnar application will inform you about this. Your microphone is then turned on only as long as you are using the relevant function in the application. If you change the function or turn it off, the microphone will turn off automatically until you want to use the function again. Application Pirnar will not prompt you again or ask you to activate the microphone if you initially granted application Pirnar access to the microphone. You can disable application's
microphone access at any time in your mobile phone settings. During the time the microphone is turned on, we will process audio recordings captured by the microphone accordingly, but only for the

purpose of performing the features you have requested. The audio recordings in question will not be permanently stored and will be deleted immediately. This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.

- Wi-Fi connection data

Our application uses your mobile device's Wi-Fi connection to connect to the internet.
This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.

- Other device functions or sensors

By accessing other features and sensors of your mobile device, our application can retrieve data from the internet and process error messages. In addition, this also allows us to start our application when the device is started and to turn off the sleep mode of the device. This is a processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you request.

Data retention period/criteria for determining the data retention period
When the device is removed from the application, the data is deleted immediately. However, the device usage history and statistics remain stored on our servers. Recordings of microphones are erased immediately.

8. Device safety, analysis and news

Device safety and troubleshooting
We process technical data about the SecuroSmart system, such as device type (reference number), serial number, error logs, version of the device software and your Pirnar application, so that we can ensure the safe operation of the devices and their compliance with new and upcoming features. This processing is intended to ensure that the application is compatible with the connected devices and that the devices operate without incompatibility-related problems. Data processing for this purpose may also include identification data, usage data and sensor data referred to in item 6.1. This data will, insofar as this is possible, be analysed in pseudonymised or anonymised form. To the extent that we can thereby ensure the operation of your Pirnar application and the connected PIRNAR entrance door with the built-in SecuroSmart system, this constitutes data processing in accordance with Article 6(1)(b) of the GDPR, as this data is necessary for the provision of the services you have requested. Analysing the data of devices for general quality improvement (and product development) constitutes our legitimate interest in accordance with Article 6(1)(f) of the GDPR. After anonymising your personal data, it is no longer possible to establish your identity. We keep the data for a period of five years in order to ensure long-term compliance and proper operation of the devices.

Usage analysis and offer expansion
If you have given us your consent (through the appropriate sliders and settings in the application), we will analyse the use of the Pirnar application, the SecuroSmart system and, if necessary, other devices that you use in order to improve our existing products, develop new products and obtain information

on which products are most wanted in certain locations and when (expansion and planning of the offer). In addition, with the help of our customers, we want to come up with general recommendations on which related products would make sense and are popular. Therefore, we analyse the registered PIRNAR entrance door with the built-in SecuroSmart system in order to learn about the popularity of products in certain customer segments and locations. We also want to compare the number, type and extent of actual use with the devices sold. The data processed for this purpose shall include, in particular, the data referred to in item 6.1, i.e. identification data, usage data, general data on the PIRNAR entrance door with the built-in SecuroSmart system and location data. The above data, when combined with the related data, shall be processed in an anonymised form. This is a processing in accordance with Article 6(1)(a) on the basis of your explicit consent. You may revoke this consent at any time with future effect. You can withdraw your consent by moving the slider in the application menu under the Settings/Opti-in tab accordingly. From this point on, your data will no longer be processed; the data that was already analysed, however, will continue to be used, mainly because it will only be available in anonymised form. If we anonymise your personal data, it is no longer possible to establish your identity. We store this data for a period of seven years so that we can follow the usual product development cycles.

Personalised news

With your explicit consent, we can send you newsletters by e-mail containing, among other things, personalised recommendations, novelties and our offers. Our product recommendations are based on which PIRNAR door with the built-in SecuroSmart system you are using and which products are generally suitable for you based on your circumstances. At the same time, we analyse usage patterns of customers who have already purchased a specific product (in case other customers using similar devices often use other similar devices, for example). In the context of advertisements for PIRNAR products that may be displayed in the application (via push notifications), personal data is not processed (these advertisements are displayed to all users of the application). The data processed for this purpose shall include, in particular, the data referred to in item 6.1, i.e. identification data, usage data, general data on the PIRNAR door with the built-in SecuroSmart system and location data. In the context of advertisements for PIRNAR products that may be displayed in the application (via push notifications), personal data is not processed (these advertisements are displayed to all users of the Pirnar application). The content may concern products, promotions, sweepstakes and novelties, but it may also include customer satisfaction surveys that we provide. The legal basis for this data processing is your consent in accordance with Article 6(1)(a) of the GDPR. Your consent to receive personalised newsletters can be revoked at any time in the application with effect for the future. Alternatively, you can click on the "Unsubscribe" link in the e-mail with the relevant newsletter. We store the above data for these purposes for a period of one year so that we can analyse your current use of our products. If you revoke your consent to receive PIRNAR news, your personal data stored for these purposes will be deleted.

9. Other functions

If you open a specific website through a browser in the Pirnar application (by clicking on a link, for example), your personal data on this website may be processed under different conditions from these data protection provisions. These data protection provisions only apply to our application. We ask you to comply with the data protection policy of the linked websites. We do not accept any responsibility for third-party content that you access through links and that is specifically marked, as this is not our content. Unlawful, incorrect or incomplete content as well as damage resulting from the use or non-use of information are the sole responsibility of the provider of the website to which the link leads.

10. Data recipient

Below we would like to inform you about the recipients of your data.

Transmission of data to contractual data processors
In the context of contractual data processing, that is on the basis of a contract and upon our order, we also partially use external service providers for data processing, subject to legal regulations, which operate in accordance with our instructions and are under our control.

The contractual data processors are in particular:
• technical service providers that help us provide services related to our Pirnar application, e.g.: maintenance services, computer centre management, web hosting; and
• technical service providers that help us provide certain functions

- Apple Inc.
- Google LLC
- Tuya Inc.

In these cases, we remain responsible for the processing of data; the transfer and processing of personal data to or from these contractors rests on the legal basis that allows us to process data in individual cases. No specific legal basis is required for this.

Disclosure of data to third parties
As described above, we may share your information with Google LLC., Amazon or Apple if you use a voice assistant (item 5.3). In addition and for internal administrative purposes, PIRNAR will pass on the information you provide when registering, including to the joint customer service department, if necessary. The possible provision of personal data is justified by our legitimate interest to transfer data within our group of companies for administrative purposes, in which case your rights and interest regarding protection of your personal data within the meaning of Article 6(1)f of the GDPR do not take precedence. Where necessary to explain the illegal use or misuse of the application or in the context of legal proceedings, personal data may be transferred to law enforcement or other public authorities, as well as to injured third parties or legal advisers where appropriate. However, this will only take place

if there is a reasonable suspicion of an illegal act or abuse. The data may also be transmitted if this is necessary for the implementation of the terms of use or other legal claims. In addition, we are required by law to provide information to certain public authorities upon request. These could be law enforcement authorities, state authorities exercising control over infringements, or financial authorities. Possible transfer of personal data is justified by the fact that (1) the processing is necessary for the performance of a legal obligation to which we are subject under Article 6(1)(c) of the GDPR in conjunction with national regulations for the transfer of data to law enforcement authorities, or (2) we have a legitimate interest in transferring the data to these third parties in the event of suspicion of misuse or for the implementation of our terms of use, other conditions or in the event of legal claims, in which case your rights and interest regarding protection of your personal data within the meaning of Article 6(1) (f) of the GDPR do not take precedence.

In the further development of our company, there may be changes in the structure of our company, whereby we might change the legal form of the company, establish subsidiaries, establish, buy or sell equity interests or parts of the company. In such cases, customer data may be transferred, where appropriate, together with the part of the company that is subject to change of ownership. In the event of transfer of personal data to third parties to the extent described above, we will ensure that this is carried out in accordance with these data protection provisions and the applicable data protection legislation. The possible provision of personal data is justified by our legitimate interest in adapting the form of our company to the given economic and legal situation, in which case your rights and interest regarding protection of your personal data within the meaning of Article 6(1)f of the GDPR do not take precedence.

11. Non-EU recipients

Technical service providers acting as contractual data processors or third parties (see item 10) are also partly located in China and the USA. In any case, we will ensure an adequate level of data protection, for example, we will conclude a contract with contractual data processors that contains standard data protection provisions of the European Commission in accordance with Article 46(2)(c) of the GDPR. In order to exercise your further rights under Article 13(1)(f) of the GDPR, you may contact us using the contact details referred to in item 14.

12. Your rights

Overview

In addition to the right to revoke the consent to the collection of personal data you have given us, you are also entitled to the following rights, if all legal conditions are met:

- the right of access to your personal data held by us in accordance with Article 15 of the GDPR,
- the right to rectification of inaccurate or incomplete data in accordance with Article 16 of the GDPR,
- the right to erasure of your personal data held by us in accordance with Article 17 of the GDPR,
- the right to restriction of processing of your data in accordance with Article 18 of the GDPR,
- the right to data portability in accordance with Article 20 of the GDPR,

• the right to object in accordance with Article 21 of the GDPR.

Right of access to data in accordance with Article 15 of the GDPR

In accordance with Article 15(1) of the GDPR, you have the right to request information about your personal data stored with us free of charge. Above all, this entails:

• the purposes for which we process your personal data,
• the categories of personal data processed,
• recipients or categories of recipients to whom the personal data in question have been or will be disclosed,
• the estimated retention period of your personal data or, if no specific answer can be given, the criteria for determining the retention period,
• the right to rectification or erasure of personal data concerning you, the right to restriction of processing by the responsible person or the right to object to the processing of data,
• the right to lodge a complaint with the supervisory authority,
• all available information on the source of the data, if the personal data are not collected directly from the data subject,
• the existence of automated decision-making, including profiling in accordance with Article 22(1) and (4) of the GDPR and - at least in such cases - meaningful information on the reasons for it, as well as the meaning and intended consequences of such processing for the data subject. Where personal data are transferred to a third country or international organization, the data subject shall have the right to be informed of appropriate safeguards relating to the transfer in accordance with Article 46.

Right to rectification in accordance with Article 16 of the GDPR

You have the right to request us to promptly correct inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to request the supplementation of incomplete personal data, including the submission of a supplementary statement.

Right to erasure in accordance with Article 17 of the GDPR

You have the right to request from us the immediate deletion of personal data concerning you, when one of the following reasons applies:

• personal data are no longer needed for the purposes for which they were collected or otherwise processed;
• you have revoked your consent on the basis of which the processing takes place in accordance with item (a) of Article 6(1) or item (a) of Article 9(2) of the GDPR, and where there is no other legal basis for the processing;
• you object to the processing of data in accordance with Article 21(1) or (2) of the GDPR, and in the case of Article 21(1) of the GDPR, there are no overriding legitimate reasons for their processing;
• personal data have been processed unlawfully;
• the erasure of personal data is necessary to fulfil a legal obligation;
• personal data were collected in connection with the offer of information society services referred to in Article 8(1) of the GDPR.

If we have publicly disclosed personal data and are obliged to delete them, we will take appropriate measures to inform third parties who process your personal data that you are also requesting from them to delete all links to or copies of these personal data, taking into account the available technology and implementation costs.

Right to restriction of processing in accordance with Article 18 of the GDPR

You have the right to request a restriction of processing from us where one of the following situations applies:

• you dispute the accuracy of personal data;
• the processing is unlawful and instead of deletion you request a restriction of the use of personal data;
• the responsible person no longer needs the personal data for the purposes of processing, but the data subject needs it in order to assert, exercise or defend legal claims; or
• the person concerned has lodged an objection to the processing in accordance with Article 21(1) of the GDPR until it is verified that the controller's legitimate reasons prevail over those of the data subject.

Right to data portability in accordance with Article 20 of the GDPR

You have the right to receive your personal data provided to us in a structured, commonly used and machine-readable form, as well as the right to transmit this data to another controller without being obstructed by the controller to whom the personal data were provided, when:

• the processing is based on consent pursuant to item (a) of Article 6(1) or item (a) of Article 9(2) or on a contract pursuant to item (b) of Article 6(1) of the GDPR; and
• the processing is carried out by automated processes.

In exercising your right to data portability, you have the right to have personal data transferred directly from us to another data controller where technically feasible.

Right to object in accordance with Article 21 of the GDPR

Under the conditions laid down in Article 21(1) of the GDPR, you may object to the processing of data for reasons arising from an emergency situation on your part.

The aforementioned general right to object applies to all purposes of data processing described in these data protection provisions, processed on the basis of Article 6(1)(f) of the GDPR. In contrast to the special right to object in the case of processing data for advertising purposes, we are, in accordance with the GDPR, obliged to implement such a general objection only if you provide us with reasons of greater importance, such as a potential danger to life or health. You can also contact the data protection officer of PIRNAR.

13. Contact person

Contact person for questions or exercising your rights regarding the protection of personal data

If you have questions regarding the website or application or the exercise of your rights in relation to the processing of your data (protection of personal data), you can contact: vop@pirnar.si or PIRNAR d.o.o., Bravničarjeva 20, 1000 Ljubljana.

Right to lodge a complaint with a supervisory authority
In addition, you have the right to lodge a complaint with the competent data protection supervisory authority at any time. For this purpose, you can contact the data protection supervisory authority with jurisdiction at the District Court in Ljubljana.

14. Contact details of the data protection officer of PIRNAR
Data protection provisions apply to the processing of data by PIRNAR, Bravničarjeva 20, 1000 Ljubljana (responsible person) and the Pirnar application. Contact person for data protection: vop@pirnar.si.

Date of last inspection: 01.06.2022
PIRNAR d.o.o.