Warsaw, date 26.06.2026

PRIVACY POLICY
for the "PIM-MC (iOS)" application

§1
General information

This Privacy Policy sets out the rules for the processing of personal data of users of the "PIM-MC" mobile application (hereinafter: the "Application"). The personal data controller is: MindMade Sp. z o.o., Plac Konstytucji 3, 00-647 Warsaw, Poland, Tax ID (NIP): 7010261220, email: biuro@mindmade.pl, hereinafter: the "Controller". The Controller takes special care to protect the privacy of users and the personal data being processed. Providing data is voluntary, but failure to provide it may make it difficult or impossible to use the application or certain functionalities thereof.

§2
Scope of data processed

1. In connection with the use of the Application, the Controller may process the following data:

1.1 User identification data

1) first and last name
2) email address
3) user identifier in the system

1.2 Data related to use of the application

1) information on the user's activity in the system
2) technical data of the device
3) data concerning use of the application's functionalities

1.3 Technical data

1) IP address
2) device type
3) operating system
4) application version
5) tokens and technical identifiers necessary to maintain the session, ensure security, and deliver push notifications, including VoIP notifications
6) technical data concerning events in the system, such as message or call identifiers, insofar as they are necessary to support the functionalities of the Application

1.4 Communication, location, and multimedia data

Depending on the service configuration and the features made available in a given deployment, the Controller may also process:

1) data concerning calls, including call history, call identifiers, information about the initiator, recipient, time, and call status;

2) user's location data, including the device's current location and location history, if location features are enabled in a given deployment;
3) messages, attachments, and files sent by users within the system;
4) audio/video data, including camera image and microphone audio, as well as audio/video recordings, if the recording feature is enabled in a given deployment;
5) data related to access to content and events in the system, in particular information on their viewing, playback, or handling by authorized users.

§3
Purposes and legal bases for data processing

1. Users' personal data is processed for the following purposes:
   1) enabling the user to use the Application and the Controller's IT system, including performing the Application's communication, dispatcher, location, and multimedia functions, as well as managing the user account and providing technical support and user assistance (Art. 6(1)(b) GDPR);
   2) analyzing (including technical and statistical analysis) use of the Application and the Controller's system, ensuring the security of the Application, the system, and their use, and developing the Application and the Controller's system, including adapting them to users' needs, based on the Controller's legitimate interest (Art. 6(1)(f) GDPR);
   3) pursuing claims and defending against claims, within the Controller's legitimate interest (Art. 6(1)(f) GDPR);
   4) fulfilling legal obligations incumbent upon the Controller, in particular obligations arising from civil, administrative, tax, or accounting law (Art. 6(1)(c) GDPR);
   5) protecting the vital interests of the user (Art. 6(1)(d) GDPR). The user's data will not be subject to profiling or automated decision-making.

§4
Source of data

1. Users' data may be obtained:
   1) directly from the user
   2) from the organization (business client) that granted the user access to the system
   3) automatically while using the Application, within the scope of technical and operational data necessary for the proper operation of the Application, ensuring security, maintaining the session, diagnosing errors, and performing the features available in the Application;
   4) through the Controller's system, in particular via the API, within the scope of the user's decisions, settings, and preferences, such as selection of system options, configuration of functionalities, acceptance of terms and conditions, or rules for use of the service. The Application does not use cookies. User settings, preferences, and decisions are stored in the Controller's system via the API and are associated with the user account to the extent necessary for the operation of the Application and the provision of the service. The Application may use technical mechanisms specific to mobile applications, such as authentication tokens, push notification tokens, technical identifiers, and local application settings, only to the extent necessary for the proper operation of the Application, session maintenance, security, and delivery of notifications.

§5
Data sharing

1. Personal data may be shared with:
1) entities providing IT services to the Controller;
2) hosting service providers;
3) entities providing technical support to the Controller;
4) other subcontractors of the Controller and other entities providing resources, including goods or services, necessary for the proper operation of the Application and the Controller's system;
5) the Controller's advisors, in particular legal, economic, and tax advisors;
6) entities authorized to receive data under applicable laws;

2. The Controller does not sell users' personal data. In a given deployment, authorized representatives of the organization that granted the user access to the Application may also have access to the user's data, in particular system administrators, dispatchers, or other persons authorized by that organization. Depending on the service configuration and permissions granted in the system, the scope of such access may include communication data, call history, location data, location history, messages, files, and audio/video recordings, if the given feature is used in the given deployment.

§6
Transfer of data outside the European Economic Area and to international organizations

1. The Application is made available to users in connection with a service provided under an agreement concluded with the organization that granted the user access to the Application. The Application may connect to servers and infrastructure appropriate for a given deployment. The location of this infrastructure depends on the service configuration and the provisions of the agreement concluded with the given organization.
2. Depending on the specific deployment, users' personal data may be processed exclusively within the European Economic Area or may be transferred to third countries, i.e., outside the European Economic Area, or to international organizations. If such data transfer occurs within a given deployment, it is carried out in accordance with the provisions of the GDPR, in particular based on a European Commission adequacy decision, standard data protection clauses, or other appropriate safeguards provided for in Chapter V of the GDPR. Detailed information on any transfer of data outside the European Economic Area or to international organizations, including the third country, international organization, data recipient, transfer basis, and safeguards used, is included in the documentation, agreement, or information clause applicable to the given deployment or the organization that granted the user access to the Application.
3. Regardless of the location of the infrastructure for a given deployment, the Application may use the Apple Push Notification service (APNs), provided by Apple, solely for the purpose of delivering push notifications on iOS devices. In this respect, technical data necessary to deliver the notification may be transferred to Apple, in particular the device/application token and a

limited notification payload. The notification payload does not contain message content and is limited to information necessary to support the given function of the Application, such as information about a new message, a missed call, a call identifier, or basic information about the call initiator in the case of VoIP notifications. Data transferred through APNs is not used by the Controller for advertising or analytics purposes.

§7
Data retention period

1. Personal data is stored for the period of:
   1) the user's use of the Application or the Controller's system
   2) the term of the agreement between the Controller and the client
   3) the period necessary to fulfill the Controller's legal obligations
   4) the expiration or limitation period of claims that may be available to the Controller or the user in connection with the processing of such data or legal relationships between them,
   5) the period necessary to pursue or defend the rights and interests of the Controller,
   6) until the user withdraws the consent granted;
   7) the period necessary for the operation of the Application's technical mechanisms, such as session maintenance, security, and error diagnostics;
2. Data is stored for the period necessary to achieve the purpose for which it was collected, and thereafter for the period required by law or necessary to establish, pursue, or defend claims. The retention period may vary depending on the category of data and the purpose of its processing.
3. After the end of the processing period, data may be deleted or anonymized to an extent that it no longer meets the definition of the user's 'personal data'.

§8
User rights

1. The user has the right to:
   1) request that the Controller provide access to that user's data, as well as receive a copy thereof (Art. 15 GDPR);
   2) request that the Controller rectify or correct that user's data (Art. 16 GDPR);
   3) request that the Controller erase that user's data (Art. 17 GDPR);
   4) request that the Controller restrict processing (Art. 18 GDPR) - e.g., when the user notices that the data is inaccurate - the user may request restriction of processing of their data for a period allowing the Controller to verify the accuracy of that data);

To exercise the above rights, the user should contact the Controller.
The user also has the right to lodge a complaint with the President of the Personal Data Protection Office in connection with the Controller's processing of that user's personal data.

§9
Data security

The Controller applies appropriate technical and organizational measures to protect the personal data being processed against loss, unauthorized access, or disclosure.

§10
Children's data

The Application is not intended for persons under 16 years of age. The Controller does not knowingly process children's personal data.

§11
Changes to the Privacy Policy

The Controller may update this Privacy Policy in the event of legal, technological, or organizational changes.
The current version of the Privacy Policy is published on the Controller's website.

§12
Contact

For matters concerning personal data protection, the Controller may be contacted at:
email: biuro@mindmade.pl