Privatewave - Information on the processing of personal data

Information on the processing of personal data pursuant to Art. 13 of the RGPD 679/2016

Dear Madam/Sir,

pursuant to art. 13 of the EU General Data Protection Regulation no. 679/2016, containing provisions on the processing of personal data (hereinafter, **RGPD**), we hereby inform you that **BV TECH S.p.A.,** as the Data Controller of the data you have provided, will use this information concerning you and, qualified as "personal data" by the RGPD. The regulation states that anyone who processes personal data must inform the person concerned of what data is processed and of certain elements qualifying the processing, which must in any case be carried out in a lawful, correct and transparent manner, protecting your confidentiality and guaranteeing your rights.

1.DATA CONTROLLER

The Data Controller is **BV TECH S.p.A.**, with registered office at Piazza Diaz 6, 20123, Milan - Italy

2. DATA PROTECTION MANAGER (RPD/DPO)

The Data Protection Manager can be contacted at the following email address: dpogruppo@bv-tech.it.

3. PURPOSE OF PROCESSING AND NATURE OF DATA

The information and personal data indicated below will be processed for the following purposes

to fulfil the execution of the contract with you for the supply and management of the following **Apps**:

- **"*PRIVATEWAVE Professional*"**
- **"*PRIVATEWAVE Enterprise***

and/or related services requested by you, namely:

1. **Telephone number** (necessary for user identification, use of the service and contact with other users);
2. **administrative information** for contract management;

optional data:

1. **Information relating to your request**, if you contact us with questions or complaints;
2. **Geographic location** of the phone. The User can transmit the coordinates of his current geographical position to his contacts if he gives the PrivateWave application the permissions to access the position information. The coordinates are transmitted in end-to-end encrypted mode and are used to display the user's position on the map. The transmitted coordinates are anonymous and do not contain any data that can personally identify the user. Thanks to the end-to-end encryption, it is not possible for the PrivateWave server to trace the user's location;
3. **Contacts in the address book.** The User can optionally provide PrivateWave with the contact list of his telephone. The contacts are cryptographically hashed and transmitted to the server. They are used only to determine which contacts are PrivateWave users. The user's contact list is not stored in any way in the Privatewave server and is not shared with third parties;
4. **Photo/video gallery**. For sending photo or video attachments in messages. PrivateWave cannot in any way access end-to-end encrypted user messages and attachments;
5. **Files on your phone**. For sending attachments in messages. PrivateWave cannot in any way access end-to-end encrypted user messages and attachments;
6. **Phone camera**. For sending photo or video attachments in messages. PrivateWave cannot in any way access end-to-end encrypted user messages and attachments;
7. **Phone microphone**:
    a. for sending audio attachments in messages. PrivateWave cannot in any way access end-to-end encrypted user messages and attachments;
    b. for communication with other users. PrivateWave uses end-to-end encryption for VoIP calls and messages. The content of calls and messages is always encrypted and cannot be revealed to anyone except the sender and recipient.

4. LEGAL BASIS FOR PROCESSING

The personal data referred to in point 3) of the information notice will be processed lawfully because the following conditions are met:

- processing is **necessary for the performance of a contract to which the data subject is party** or for the performance of pre-contractual measures taken at the request of the data subject (art. 6, par.1, letter b RGPD);
- processing is **necessary for the purposes of pursuing the legitimate interests of the Data Controller** (Art. 6(1)(f) GDPR).

5. OBLIGATION OR FACULTY TO PROVIDE DATA AND CONSEQUENCES OF REFUSAL TO DO SO

The provision of data is necessary for the establishment and management of the contractual relationship. We inform you that, in the absence of such data, it will be impossible for our Company to fulfil the obligations of the contract in place with you. Therefore, failure to provide such data will make it impossible to establish or continue the contractual relationship to the extent that such data are necessary for us to correctly fulfil the obligations related to the management of the contract.

6. STORAGE

Personal data in the *rendez-vous* cloud solution will be stored in the PrivateWave infrastructure in compliance with the conservation limitation principle provided for by the RGPD and/or for the time necessary to pursue the purpose of the service and for legal and / or contractual obligations.

Encrypted messages and their attachments are temporarily queued on the server to be delivered to recipient devices that are temporarily offline. PrivateWave cannot access end-to-end encrypted user messages in any way. The personal data for the *on-premise* solution are within the customer's infrastructure and therefore in the responsibility of the latter.

7. SECURITY MEASURES

We comply with all industry standard measures aimed at eliminating the risk of damage and unauthorized access or use of personal information, ensuring that we have implemented adequate technical and organizational policies to apply the security measures established by the RGPD.

PrivateWave uses open protocols and IETF standards and complies with the NSA mobility capability package for the protection of National Security Systems (NSS).

All data is transmitted using the HTTPS protocol encrypted with TLS stack at the highest certification level (ECDHE-AES256-SHA384-GCM). PrivateWave encrypts in end-to-end (ZRTP ECDH 384/512) or end-to-site (SDES) mode even all data (Voice, messages and attachments) before they leave the phone, with a key that only the other recipient phone knows.

The content of calls and messages cannot be revealed to anyone except the sender and recipient. Any communication between client and server is also encrypted.

Privatewave immediately realizes if a *man-in-the-middle* attack attempt is in progress, warning the user and immediately closing any type of communication. All data on the mobile device is stored in an encrypted database with an access PIN chosen by the user and which not even PrivateWave knows. The data is kept for the period of time that the user deems appropriate.

8. DATA PROCESSING METHODS AND RECIPIENTS

Your personal data will be processed both by the **Company's staff, authorised to process** them using electronic and paper-based instruments, and by **ex ternal parties** (collaborators and service providers) called upon to carry out specific tasks on behalf of the Data Controller, in their capacity as **Data Processors**, pursuant to art. 28 RGPD, subject to our letter of appointment imposing on them the duty of confidentiality and security in the processing of personal data, and with the adoption of suitable security measures to prevent loss and/or unlawful and incorrect use of the data and/or unauthorised access, in compliance with the provisions in force on the protection of personal data.

Below is a list of our service providers:

- **Vonage Holdings Corp** provides SMS service for first installation.

  For more information, visit their privacy policy: https://www.vonage.com/legal/privacy-policy/?icmp=footer_legalpolicy_privacy

- **Swisscom Holdings Corp** (LogMeIn) provides some cloud hosting services for the rendezvous solution.

  For more information, visit their privacy policy: https://www.swisscom.ch/en/business/footer/data-protection.html

- **Firebase** (Google LLC) provides push notification services.

  For more information, visit their privacy policy: https://firebase.google.com/support/privacy

- **Apple Inc.** provides push notification services.

  For more information, visit their privacy policy: https://www.apple.com/ca/legal/privacy/en-ww/

Instead, for the sake of brevity, the detailed list of authorized subjects and collaborators designated as Data Processors is available at the headquarters of the Data Controller and is at your disposal.

9. TRANSFER, DISSEMINATION AND COMMUNICATION OF DATA

The processed data will **not be transferred** to third countries or international organizations, will not be disseminated, and will not be communicated to third parties except, where necessary, for legal and/or contractual obligations.

10. RIGHTS OF THE INTERESTED PARTY

As envisaged by the RGPD, in relation to your data you are entitled to exercise the rights envisaged by articles 15 et seq. of the RGPD, as set out below, and more precisely

- **"right of access"** in order to obtain confirmation from the Data Controller as to whether or not data is being processed personal data concerning you, and if so, to obtain access to the personal data and to the following information: a) to know the purposes of the processing; b) the categories of personal data being processed; c) the recipients or categories of recipients to whom the data have been or will be communicated, in particular if they are recipients from third countries or international organizations; d) where possible, the expected data retention period or the criteria used to determine this period; e) if the data are not collected from the data subject, to obtain all available information on their origin;
- **"right to rectification**" to obtain the rectification of data relating to you;
- **"the "right to erasure/oblivion"** to obtain the erasure of data concerning you in the cases

provided for by law;

- **"right to restriction of processing"** to obtain restrictions on processing in the cases provided for by law;
- **"right to data portability"** to obtain the portability of the data, i.e. to receive them from a Data Controller in a structured, commonly used and machine-readable format and to transmit them to another data controller without hindrance in the cases provided for by law;
- **"right to object"** to object to the processing at any time in the cases provided for by law;
- **"right to be informed"** of the existence of an automated decision-making process concerning natural persons, including profiling;
- **"right to lodge a complaint with a Supervisory Authority"** ex art. 77 RGPD (Data Protection Authority).

Please note that there may be conditions or limitations to the rights of the data subject. It is therefore not certain that, for example, you can exercise your right to data portability in all cases. This depends on the specific circumstances of the processing activity, or, if you decide to object to the processing of your data, the Data Controller has the right to evaluate your request, which may not be accepted if there are compelling legitimate grounds to proceed with the processing that override your interests, rights and freedoms.

11. METHODS OF EXERCISING YOUR RIGHTS

Without any formality, the data subject may at any time exercise his/her rights in a clear and explicit manner by sending:

- an email or **by contacting the DPO/DPO**: dpogruppo@bv-tech.it - +39 02/85.96.171
- by contacting the Controller directly by sending:
- a registered letter with acknowledgment of receipt to the BV TECH S.p.A. Piazza Diaz 6, 20123 – Milan - Italy
- an e-mail to: info@bv-tech.it.

Last update: Milan 14 March 2021