Privacy Policy pursuant to Article 13 of (EU) Regulation No. 679/2016 (“GDPR”)

-APP MOBILE-

Aruba S.p.a. (hereinafter "Aruba") protects the confidentiality of personal data and guarantees its necessary protection against any event that may put it at risk of violation.

As provided for by European Union Regulation No. 679/2016 (hereinafter “GDPR”) and Article 13 in particular, please find below the information required by law relating to the processing of your personal data.

SECTION I

Who we are and what data we process (Article 13, paragraph 1 (a), Article 15 (b) GDPR)

Aruba S.p.a., represented pro tempore with registered offices at Via San Clemente, 53 Ponte San Pietro (BG) Italy, acts as the Data Controller and can be reached at privacy@staff.aruba.it and collects and/or receives information relating to you, such as:

Category of data	**Examples of types of data**
Identification data	First name, last name, physical address, nationality, residential province and city, landline telephone number and/or cell number, fax, tax ID number, email address(es), images/sounds.
Banking information	IBAN and banking/postal account information (except for Credit Card number)
Internet traffic data	Logs, originating IP address

Furthermore, when using individual Applications ("**Apps**"),and exclusively for purposes of service provision requirements, during first use of the required functionality, each App will ask permission to access certain functions offered by the operating system that you use, which may also be denied/granted from the operating system's settings. In particular:

Device resources and data being processed	**Purposes**
Access to the notification system (depending on the type of operating system used, through the user account)	Sending of notifications
Access to address book	Retrieval of contacts' email addresses
Access to the photo library	Downloading and/or saving attachments
Access to document folders	Downloading and/or saving attachments
Access to camera and voice/audio devices and/or settings	Downloading attachments, QR code activations, managing video calls
Identification data for the mobile device (such as telephone number, IMEI code), network information, device status and functionality, accounts available on the device	Managing notification functions (sounds, vibration, brightness, etc.), security verifications.
Enabling the app to receive text messages	Reading authentication messages
Access to network information and connection status	Server connection and background management

Aruba *does not* require you to supply so-called "private" data, that is, according to the provisions of the GDPR (Art. 9), personal data that identifies race or ethnicity, political opinions, religion or philosophy, or any union affiliation, nor any genetic or biometric information used to uniquely identify a physical person, data associated with health or one's sex life, or sexual orientation. In the event the services requested from Aruba require the processing of this data, you will first receive specific notification with a request for your consent.

During their normal operation, computer systems and software applications involved in the downloading/functioning of Apps (including, but not limited to, Apple Store, Google Play and Windows Phone Store) collect some of the user's data, the transmission of which is an inherent part of using internet communication protocols and the smartphones and devices used, and which, in any case, are processed by the relevant Managers as independent Data Controllers.

The Data Controller has nominated a Data Protection Officer (DPO) who can be contacted for any information or requests:

email: dpo@staff.aruba.it

Telephone number : +39 0575/0505

For any information or requests, please contact the following address

privacy@staff.aruba.it

Telephone number +39 0575/0505

SECTION II

Why we need your data (Art. 13, paragraph 1 GDPR)

Data are used by the Data Controller to execute the download request, to activate and provide the Application chosen by you and to ensure the proper functioning and use of its features, manage and execute access/login and contact requests sent by you, offer assistance, and fulfil the legal and regulatory obligations required of the Data Controller in accordance with the activities performed. In no case will Aruba resell any of your personal information to third parties nor use it for any purpose not stated.

The legal basis for this processing is to provide the services relating to the request for activation and provision of the App, information and contact, and/or the sending of informational materials, and to comply with legal requirements.

digital security

In line with the provisions of Clause 49 of the GDPR and through its providers (third parties and/or recipients), the Data Controller processes your personal traffic data only to the extent strictly necessary and proportionately in order to guarantee the security of the networks and the information. This means the capacity of a network or information system to block, at a given level of security, any unforeseen events or illegal or malicious acts that would compromise the availability, authenticity, integrity and confidentiality of the personal data stored or transmitted.

The Data Controller will immediately notify you if there is any risk of violation of their data, except for any obligations noted in the provisions of Art. 33 GDPR associated with notifications of personal data violations.

The legal basis for this processing is to comply with legal requirements and the legitimate interests of the Data Controller in undertaking processing for the purpose of protecting corporate assets and the security of the Aruba Group's offices and systems.

fraud prevention (Clause 47 and Art. 22 of the GDPR)

- except for special category data (Art. 9 GDPR) or data relating to criminal convictions and offences (Art.10 GDPR), your personal data will be processed to allow controls for the purposes of monitoring and preventing fraudulent payments. This processing will be undertaken by software systems that run automated checks and will be carried out prior to negotiating Services/Products;
- a negative result from these checks will render the transaction impossible; you can, of course, express your opinion, obtain an explanation, or dispute the decision by outlining your reasons to the Customer Care Department or to privacy@staff.aruba.it;
- personal data collected only for anti-fraud purposes, which differs from the data needed for the proper performance of the service requested, shall be immediately deleted upon termination of the verification phase.

protection of minors

The Services/Products offered by the Controller are reserved for those entities legally able, based on national regulations, to satisfy contractual obligations.

To prevent illegal access to its services, the Data Controller implements preventive measures to protect its own interests, such as checking tax identification numbers and/or performing other checks, when necessary for specific Services/Products, with regard to the accuracy of the identification data on the identification documents issued by the applicable authorities.

Communication to third parties and categories of recipients (Article 13, paragraph 1 GDPR)

Your personal data is communicated mainly to third parties and/or recipients whose activity is necessary to perform the activities relating to the contract established, and to meet certain legal requirements, such as:

Categories of recipients	**Purposes**
Companies belonging to the Aruba S.p.A. Group ("Aruba Group")	Fulfillment of administrative and accounting requirements as well as those connected with the contractual services,
Third party providers and companies belonging to the Aruba S.p.A. Group*	Performance of services (assistance, maintenance, delivery/shipping of products, performance of additional services, providers of networks and electronic communication services) associated with the requested service
Credit and electronic payment institutions, banks/post offices	Managing deposits, payments, reimbursements associated with the contractual service
External professionals/consultants and consulting firms	Fulfillment of legal requirements, exercising rights, protecting contractual rights, credit recovery
Financial Administration, Public Agencies, Legal Authorities, Supervisory and Oversight Authorities	Fulfillment of legal requirements, protection of rights; lists and registries held by Public Authorities or similar agencies based on specific regulations relating to the contractual service
Formally mandated subjects or those with recognized legal rights	Legal representatives, administrators, guardians, etc.

***** The Controller requires its own third party providers and Data Processors to adhere to security measures that are equal to those adopted for you by restricting the Data Processor's scope of action to processing directly related to the requested service.

The Data Controller will not transfer your personal data to countries where the GDPR is not applicable (countries outside the EU) except where specifically indicated otherwise, in which case you will be notified in advance, and if necessary asked for your consent.

The legal basis for this processing is fulfillment of the services outlined in the established contract, compliance with legal obligations, and the legitimate interests of Aruba S.p.a. to perform the processing necessary for these purposes.

SECTION III

What happens when you do not provide your identification information as needed to perform the requested service? (Article 13, paragraph 2 (e) GDPR)

The collection and processing of your personal data is necessary to fulfill the service requests as well as to perform the Service and/or supply the requested Product. Should you fail to provide your personal data as expressly required within the order form or the registration form, the Data Controller will not be able to carry out the processing associated with managing the requested

services and/or the contract and the Services/Products associated with them, nor fulfill the operations dependent on them. In particular, refusal to grant the App access to one or more resources of the mobile device and/or its data, depending on the type of App chosen, may result in your not being able to use all or part of the related App functions.

How we process your data (Article 32, GDPR)

The Controller makes use of appropriate security measures to preserve the confidentiality, integrity and availability of your personal data, and requires the same security measures from third party providers and the Processors.

Where we process your data

Your data is stored in hard copy, electronic and remote archives located in countries where the GDPR is applicable (EU countries).

How long is your data stored? (Article 13, paragraph 2 (a) GDPR)

Unless you explicitly express your own desire to remove it, your personal data will be stored until required for the due purposes for which it was collected.

In particular, data will be stored for the entire duration of the provision of the App that you have installed.

It is also important to add that, should the user forward to Aruba personal data that has not been requested or that is unnecessary for the purposes of performing the services requested, or for the performance of services strictly connected thereto, Aruba cannot be considered controller of this data and will proceed to delete it as soon as possible.

Furthermore, personal data will in any case be stored to comply with obligations (e.g. tax and accounting purposes) which may continue even after termination of the contract (Art. 2220 Civil Code); for these purposes, the Controller shall retain only the data necessary to complete these activities.

In cases where it is necessary for the rights arising out of the relationship established to be used in the courts, your personal data, exclusively required for these purposes, shall be processed for the time necessary for completing them.

What are your rights? (Articles 15 - 20 GDPR)

You have the right to obtain the following from the Data Controller:

a) confirmation on whether your personal data is being processed and if so, to obtain access to your personal data and the following information:

1. the purposes of the processing;
2. the categories of personal data in question;
3. the recipients or categories of recipients that have received or will receive your personal data, in particular if these recipients are in third party countries or are international organizations;
4. when possible, the anticipated storage period of your personal data or, if not possible, the criteria used to determine this period;
5. whether you have the right to ask the Data Controller to correct or delete your personal data or the limits on processing your personal data or to oppose the processing of the data;
6. the right to lodge a complaint with a supervisory authority;
7. in the event the data is not collected from you, all of the information available regarding its origin;
8. whether there is an automated decision process, including profiling, and, at least in these cases, significant information on the logic used, as well as the importance and consequences to you for this processing.
9. the suitable guarantees provided by the third party country (outside EU) or international organization to protect any transferred data

b) the right to obtain a copy of the personal data processed, again given that this right does not affect the rights and freedoms of others; for extra copies requested by you, the Data Controller may assign a reasonable fee based on administrative costs.

c) the right to edit any of your incorrect personal data from the Data Controller without unjustified delay

d)the right to have your personal data deleted by the Data Controller without unjustified delay, if there are the reasons outlined in the GDPR, Article 17, including, for example, if the data is no longer needed for processing or if the data is considered illegal, and again, if there are no conditions outlined by law; and in any case, if the processing is not justified by another equally legitimate reason;

e) the right to obtain limits on the processing from the Data Controller, in those cases outlined in Art. 18 of the GDPR, for example where you have disputed the correctness, for the period necessary for the Data Controller to verify the data's accuracy. You must be notified, within an appropriate time, even when the suspension period has passed or the cause of limiting the processing has been eliminated, and therefore the limitation itself has been withdrawn;

f) the right to obtain information from the Data Controller on the recipients who have received the requests for any corrections or deletions or limits on the processing implemented, except when this is impossible or would create a disproportionate effort.

g) the right to receive your personal data in a structured format, commonly used and readable by automatic devices as well as the right to forward this data to another Data Controller without obstruction from the original Data Controller, in those cases outlined by Art. 20 of the GDPR, and the right to obtain direct forwarding of your personal data from one Data Controller to another, if technically feasible.

For further information and to send your request, contact the Data Controller at privacy@staff.aruba.it . To guarantee that the rights noted above are exercised by you and not by unauthorized third parties, the Data Controller may require you to provide other information necessary for this purpose.

How and when can you oppose the processing of your personal data? (Art. 21 GDPR)

For reasons associated with your particular situation, you may at any time oppose the processing of your own personal data if it is based on legitimate reasons or if it is done for business promotional activities, by sending a request to the Data Controller at privacy@staff.aruba.it.

You have the right to have your own personal data deleted if the Data Controller has no legitimate reason prevailing over such request, and in any case, where you have opposed the processing for business promotional activities.

Who can you lodge a complaint with? (Art. 15 GDPR)

Without prejudice to any other ongoing administrative or judicial action, you may lodge a complaint with the applicable supervisory authority of the Italian territory (Italian Personal Data Protection Authority), that is, with the agency that performs its duties and exercises its rights within the member country where the GDPR violation occurred.

Any updates to this information shall be communicated in a timely manner and through suitable means, and will be notified to you if the Data Controller processes your data for purposes other than those outlined in this privacy policy prior to proceeding and after you have given your consent, if necessary.