Privacy Policy pursuant to Articles 13 and 14 of Regulation (EU) 2016/679

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 (the "Regulation"), Aruba S.p.A. ("Aruba" or "Data Controller"), hereby provides below to its customers, including potential customers, as well as third parties in general (e.g. delegates, legal representatives, etc.) who come in contact with Aruba on behalf of or as mandated by customers, including potential customers (the "Data Subjects"), the information required by law relating to the processing of their personal data ("Data").

ABOUT US

Data Controller	Aruba S.p.A., with registered office in Ponte San Pietro (BG) at Via San Clemente No. 53 privacy@staff.aruba.it
Data Protection Officer (DPO)	dpo@staff.aruba.it

HOW WE COLLECT PERSONAL DATA

The data processed by the Data Controller are acquired as follows:

- from the Data Subject, also through remote communications techniques used by the Data Controller (e.g. websites, smartphone and tablet apps, call centres, etc.);
- from third parties (e.g. those arranging transactions for the Data Subject, business information etc.).

Data from public sources, such as public registers, lists, public domain documents (e.g. information contained in the register of companies at the Chambers of Commerce,

WHAT DATA DO WE PROCESS

CATEGORY OF DATA	EXAMPLES OF TYPES OF DATA
Personal information	Name, surname, street address, nationality, province and municipality of residence, landline and/or mobile phone number, , taxpayer ID number, email address, the details of identity document of which a copy is acquired where applicable .
Banking information	IBAN and banking/postal account information (except for Credit Card number).
Log	Source IP address, Log (system and network)
Internet traffic Data	In case of Mail or Connectivity Services: Data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

WHY ARE THE DATA SUBJECT'S DATA NEEDED

PURPOSES OF THE PROCESSING	LEGAL BASIS
Registration and management of contact requests and/or information materials The Data Subject's personal data are processed to implement preliminary actions and those following a registration request, to manage information and contact requests, and/or to send informational materials, as well as to satisfy any and all other obligations arising herewith.	The legal basis for this processing is to provide the services relating to a request for registration, information and contact and/or to send information materials and to comply with legal requirements. The provision of the data is optional. However if the Data Subject refuses to provide the data, it will not be possible for the Data Controller to provide the requested service.
Management of the contractual relationship The Data Subject's personal data are processed to implement actions in preparation of and following the purchase of a Service and/or a Product, such as management of the relevant order, provision of the Service itself and/or production and/or shipping of the purchased Product, related invoicing and payment management, handling of any claims and/or notifications to the	The legal basis for this processing is to provide the services relating to the pre-contractual and contractual relationship and to comply with the legal requirements. The provision of the data is optional. However if the Data Subject refuses to provide the data, it will not be possible for the Data Controller to provide the requested service.

support service and provision of the support itself, sending communications for information as well as fulfilment of any and all other obligations arising from the contract.	
Defending a right in court or out of court The Data Subject's personal data are processed to ascertain, exercise or defend a right of the Data Controller and/or to defend itself against third party claims, in court or out of court.	The legal basis of the processing is the pursuit of the legitimate interest of the Data Controller, given the balance of the rights of the latter and the Data Subject.
Information Security The Data Subject's personal data are processed to ensure network and information security, the protection of corporate assets and corporate systems.	The legal basis for this processing is compliance with the law and the pursuit of the legitimate interest of the Data Controller, given the balance of rights of the latter and the Data Subject. The Data Subject has the right to object at any time to the processing of their personal data for the purpose in question, on grounds relating to their personal situation.
Fraud prevention The Data Subject's personal data are processed to allow controls that monitor and prevent fraudulent payments by software systems running automated checks, prior to the negotiation of Services/Products. If these checks return a negative result it will be impossible to complete the transaction; the Data Subject can, of course, express their opinion, request an explanation, or challenge the decision by sending their reasons to Customer Support or to privacy@staff.aruba.it.	The legal basis of the processing is the pursuit of the legitimate interest of the Data Controller, given the balance of the rights of the latter and the Data Subject. The Data Subject has the right to object at any time to the processing of their personal data for the purpose in question, on grounds relating to their personal situation.
Promotional activities for Services/Products similar to those purchased The Data Subject's personal data are processed in order to send emails relating to promotions and offers relating to the Data Controller's Services/Products identical and/or similar to those covered by the current contract with the Data Subject, unless the Data Subject objected to the processing, initially or during subsequent communications.	The legal basis for the processing is the Data Controller's legitimate interest in promoting products or services analogous which may reasonably be of interest to the Data Subject, given the balance of the rights of the latter and the Data Controller. The Data Subject has the right to object at any time to the processing of their personal data for the purpose in question, on grounds relating to their personal situation.
Promotional activities for Services/Products offered by Aruba and Aruba Group Companies The Data Subject's personal data are processed by the Data Controller with specific consent for sending out newsletters and communications of offers, discounts and promotions of its own Services/Products and those of the Aruba Group companies through traditional methods (e.g. ordinary mail, telephone calls with operator) and/or automated methods (e.g. e-mail, SMS, instant messaging, pre-recorded phone calls).	The legal basis of this processing is the consent initially granted by the Data Subject for the processing itself, which may freely be withdrawn at any time, without prejudice to the lawfulness of any previous processing. If the Data Subject refuses to give their consent, it will not be possible to use the relevant services, without this entailing detrimental consequences for the contractual relationship with the Data Controller.
Taking part in surveys/research The Data Subject's personal data are processed by the Data Controller with specific consent, for inviting participation in surveys and market research, using traditional methods (e.g. ordinary mail, telephone calls with operator) and/or automated methods (e.g. e-mail, SMS, instant messaging, pre-recorded phone calls).	The legal basis of this processing is the consent initially granted by the Data Subject for the processing itself, which may freely be withdrawn at any time, without prejudice to the lawfulness of any previous processing. Any refusal of consent by the Data Subject makes it impossible to use the relevant services, without this having detrimental consequences for the contractual relationship with the Data Controller.
Profiling The Data Subject's personal data are processed by the Data Controller with specific consent, for profiling purposes such as the analysis of the transmitted data and the purchased Services/Products in order to offer advertising messages and/or business deals that are aligned with user selections.	The legal basis of this processing is the consent initially granted by the Data Subject for the processing itself, which may freely be withdrawn at any time, without prejudice to the lawfulness of any previous processing. If the Data Subject refuses to give their consent, it will not be possible to use the relevant services, without this entailing detrimental consequences for the contractual relationship with the Data Controller.

TO WHOM DO WE COMMUNICATE THE DATA SUBJECT'S DATA

CATEGORIES OF RECIPIENT	PURPOSE
Companies belonging to the Aruba S.p.A. Group ("Aruba Group")	Fulfilment of administrative and accounting requirements, as well as those connected with the services requested
Third party providers and companies belonging to the Aruba Group	Performance of services (assistance, maintenance, delivery/shipping of products, performance of additional services, providers of networks and electronic communication services, promotional/advertising activities only if the Data Subject has provided specific consent to marketing) 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	Fulfilment of legal requirements, exercising rights, protecting contractual rights, credit recovery
Financial Administration, Public Agencies, Legal Authorities, Supervisory and Oversight Authorities	Fulfilment of legal requirements, defence of rights; lists and registers held by Public Authorities or similar agencies based on specific regulations relating to the requested service
Formally mandated subjects or those with recognized legal rights	Legal representatives, administrators, guardians, etc.

Persons belonging to these categories operate independently as separate data controllers or as data processors appointed by the Data Controller. The Data Controller's personnel that are specially authorised for processing, including interns, temporary workers, consultants, may also have knowledge of the data, in relation to the performance of their assigned tasks. In no case shall personal data be disclosed and they shall not, therefore, be accessible by undefined parties, in any form, for example by them being made available or subject to consultation.

HOW WE PROCESS THE DATA SUBJECT'S DATA

The data shall be processed using manual, electronic and remote means and in accordance with the requirements set by the relevant legislation, which seeks to ensure the confidentiality, integrity and availability of the Data, and to avoid material or moral damages.

WHERE WE PROCESS THE DATA SUBJECT'S DATA

The Data Subject's data is stored in archives located in European Union countries. Where necessary for the pursuit of the stated purposes, the Data Subject's Data may be transferred abroad, to countries/organizations outside the European Union guaranteeing a level of personal data protection deemed adequate by the European Commission by its own decision or, otherwise, on the basis of other appropriate safeguards, such as the Standard Contractual Clauses adopted by the European Commission or the Data Subject's consent. The Data Subject is entitled to obtain a copy of any appropriate safeguards, as well as the list of countries/organizations to which the data has been transferred by writing to privacy@staff.aruba.it.

HOW LONG WE RETAIN THE DATA SUBJECT'S DATA

The Data are stored in a form which enables the Data Subject to be identified for no longer than is necessary for the collection purposes, given the laws covering the activities and sectors in which the Data Controller operates.
The Data necessary to comply with tax and accounting obligations are retained for 10 years from the termination of the contract (art. 2220 of the Civil Code).
The Data related to unpaid or canceled or unfinished order requests are retained for 3 months.
In case of Mail or Connectivity Services the internet traffic data are retained for 6 years.
The contact Personal data are processed for promotional activities as well as for participation in surveys and market research, for up to 24 months from the termination of the contract, unless prior consent is revoked by the data subject.
Contact details are processed to send commercial offers in line with the choices of the data subjects for up to 12 months from the date of termination of the contract, unless the data subject withdraws consent beforehand.

Furthermore, the processed Data:

- as part of the marketing activities, are stored for this purpose for 24 months;
- for profiling purposes, are kept for 12 months.

Once the periods thus established have transpired, the Data will be deleted or processed anonymously, unless further retention is necessary to comply with obligations or to comply with orders issued by Public Authorities and/or Supervisory Bodies.

WHAT ARE THE DATA SUBJECT'S RIGHTS

The Data Subject shall contact privacy@staff.aruba.it to exercise the right to obtain, in the cases provided for in the Regulation, access to the data concerning him/her, deletion of the data, correction of incorrect data, completion of incomplete data, limitation on processing the data, portability of the data and opposition to the processing.

The Data Subject also has the right to lodge a claim with the competent Italian supervisory authority (Italian Personal Data Protection Authority) or with the agency performing its duties and exercises its rights in the member State where the breach occurred, as provided for in Art. 77 of the Regulation, as well as to file appropriate legal proceedings pursuant to Arts. 78 and 79 of the Regulation.

Privacy Policy for Swite

In addition to the above, in the event of Swite Service the information required by law relating to the processing of personal data is provided below. t should be noted that as part of any process of interaction with the so-called "social network(s)" previously chosen by the Data Subject for importing of content via the Service(s), the Data Controller, on the basis of the settings and authorisations given independently by the Data Subject to the social network chosen by him/her, will import various types of content present within the Data Subject's account onto the aforementioned social network. The client API uses the "social network" API services, for information purposes, the main information regarding the "social network" services used for these functions is shown below:

SERVICE NAME	REFERENCE INFORMATION	INSTRUCTIONS ON HOW TO DISABLE FEATURES
YouTube API Services	http://www.google.com/policies/privacy	https://security.google.com/settings/security/permissions
Facebook Platform Graph API	https://www.facebook.com/policy.php	https://www.facebook.com/settings?tab=applications
Instagram Platform Graph API	https://help.instagram.com/519522125107875	https://www.instagram.com/accounts/manage_access/
Twitter Developer Platform API	https://twitter.com/privacy	https://twitter.com/settings/applications

When registering or linking a social media site, the Data Subject accepts permissions that authorise the importing of certain types of content. Depending on the social networks, the permissions provided, and the presence or absence of the data, Aruba imports the following categories of data:

WHAT DATA DO WE PROCESS?

CATEGORY OF DATA	EXAMPLES OF TYPES OF DATA
Data linked to the account (Profile, Page, Channel)	Account Name, Account Description, Avatar Photo, Cover Photo, Contact Information (Address, Telephone, Email), Timetable
Data on individual content	Photos, posts, tweets, videos, events, and/or reviews that the Customer has uploaded to social media or shared on their feed (if the original author of the content allows the importing of data)
Metadata linked to individual content	Title, description, link, thumbnail photo, upload date, rental tag, playlist or gallery to which it belongs

These data are used exclusively for creating and updating the Data Subject's website. Permission can be directly withdrawn via the social media platform by following the links in the table above. Revoking permissions blocks the importing of new content, but does not guarantee deletion of all the data already imported. To delete data on Data Controller (and permission):

- For a single social media network, unlink that network from the "Social Media Connected" page
- For all social networks linked to a site, delete the site from the "Site Setup" page
- For all social media sites linked to an account, delete the account from the "Account Settings" page.

Privacy Policy for E-Security services / products

In addition to the above, in the event of "E-Security" Services/ Products, presented at www.pec.it, the information required by law relating to the processing of personal data is provided below.

ABOUT US

Joint Data Controllers	Through its pro tempore legal representative, Aruba S.p.A., with registered office in Ponte San Pietro (BG) at Via San Clemente No. 53 Through its pro tempore legal representative, Aruba PEC S.p.A., with registered office in Ponte San Pietro (BG) at Via San Clemente No. 53 privacy@staff.aruba.it
Data Protection Officer (DPO)	dpo@staff.aruba.it

WHAT DATA DO WE PROCESS?

CATEGORY OF DATA	EXAMPLES OF TYPES OF DATA
Personal information	In case of Digital Signature Service and/or qualified certificates: Data and registration documents of the Service applicant, qualified certificate data and data contained in the qualified certificate, audit log and certificate life cycle. Requests to issue certificates and documents provided by the applicants, data contained in the qualified certificate, public keys provided by the applicants and personal information of the applicants and holders (in the event of being different parties); results of checks performed by the CA; Certificate suspension or revocation requests.
Log	In case of Digital Signature Service and/or qualified certificates and/or Digital Preservation: Control Journal (Audit Log), originating IP addresses associated with compilation of the remote form and the logs on the associated transactions. In case of Certified Email Service: Certified email messages log, Certified email messages log with viruses.
Images and sounds	In case of Digital Signature Service or Certified Email Service: Audio-video footage for remote visual identification. The processing of personal data contained in the audio-video footage for remote visual identification for the Digital Signature Service is carried whit specific consent of the Data Subject, expressed prior to the video recording.
Internet traffic Data	In case of Certified Email Service: Data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

HOW LONG WE RETAIN THE DATA SUBJECT'S DATA

In the case of Certification Authority Services (Digital signature, qualified certificates), Data and registration documents of the Service applicant, the audio-video footage in case of remote visual identification, qualified certificate data and data contained in the qualified certificate, the data from the audit log and the certificate life cycle are retained for 20 years from the termination of the contract.
In the case of a Qualified Electronic Time Validation Service, the logs (electronic registers) of the time validations issued are retained for 30 years unless a specific contractual agreement establishes a different duration, in any case always equal to or greater than the 20 years required by law.
In case of Certified Email Service:

- The Data Subject's personal data, any documents and audio-video footage for remote visual identification are retained for 10 years from the termination of the contract.
- Internet traffic data are retained for 6 years.
- Certified email messages log and Certified email messages log with virus are retained for 30 months.
- The access data relating to the Certified Email Service by the holder are retained for 6 months.
- The personal data of the holder of the Certified Email Service mailbox and the name of the related mailbox are not subject to deletion in accordance with the provisions of Agid.

Once the periods thus established have transpired, the Data will be deleted or processed anonymously, unless further retention is necessary to comply with obligations or to comply with orders issued by Public Authorities and/or Supervisory Bodies.

Privacy Policy for SSL Server and Code Signing Certificates

In addition to the above, in the event of Services relating to the supply of SSL Server and Code Signing Certificates, the information required by law relating to the processing of personal data is provided below.

ABOUT US

Joint Data Controllers	Through its pro tempore legal representative, Aruba S.p.A., with registered office in Ponte San Pietro (BG) at Via San Clemente No. 53 Through its pro tempore legal representative, Actalis S.p.A., with registered office in Ponte San Pietro (BG) at Via San Clemente No. 53 privacy@staff.aruba.it
Data Protection Officer (DPO)	dpo@staff.aruba.it

WHAT DATA DO WE PROCESS?

CATEGORY OF DATA	EXAMPLES OF TYPES OF DATA
Personal information	Requests to issue certificates and documents provided by the applicants, data contained in the qualified certificate, public keys provided by the applicants and personal information of the applicants and holder (in the event of being different parties); results of checks performed by the CA; Certificate suspension or revocation requests
Log	Originating IP addresses associated with compilation of the remote form and the logs on the associated transactions

HOW LONG WE RETAIN THE DATA SUBJECT'S DATA

The applicant's registration data and documents, the certificate data, the data contained therein and the life cycle of the same are retained for 20 years from the termination of the contract.
Once the periods thus established have transpired, the Data will be deleted or processed anonymously, unless further retention is necessary to comply with obligations or to comply with orders issued by Public Authorities and/or Supervisory Bodies.