Agreement pursuant to Article 28 of Regulation (EU) 2016/679 between the Customer (hereinafter the "Controller") and Qcom SpA (hereinafter the "Processor")

1. Services for which Qcom acts as Processor

For the following services, which require the processing of personal data on behalf of the Customer, Qcom acts as Processor:

Service	Processing carried out on behalf of the Customer	Personal data processed
Cloud Virtual Server	Processing (mainly storage) of any personal data residing on the virtual server	Not known
Email	Processing (mainly storage) of any personal data residing on the mail server	Not known
Managed hosting	Processing (mainly storage) of any personal data residing on the customer's hosted website	Not known
Cloud Garage	Processing (mainly storage) of any personal data residing in the cloud space provided	Not known
Cloud Backup	Processing (mainly storage and copying) of any personal data residing in the cloud space provided	Not known
Cloud secure box and secure box	Processing (mainly storage and copying) of any personal data residing in the cloud space provided	Not known
Virtual PBX phone system	Processing (mainly storage) of data relating to incoming and outgoing calls	Telephone traffic data
Newsletter	Processing (mainly sending and storage) of newsletters and promotional communications	Recipients' email addresses provided by the Customer
Online advertising campaigns and web marketing	Processing (mainly collecting contacts and sending promotional communications), also carried out as administrator of the Customer's "social" profile	Email addresses, telephone numbers, contacts on platforms acquired on behalf of the Customer or provided by the latter

2. Obligations of Qcom

Qcom, as Processor, complies with the following:

- not to communicate personal data to third parties in any way or use them for other purposes, and in any case to keep the data processed and the types of processing carried out strictly confidential. These obligations are to be considered fully in force even after the termination of this contractual relationship;
- not to transfer the data in any way to a non-EU country and, should this prove necessary, to inform the Controller of the solutions adopted in compliance with the regulatory requirements;
- to adequately instruct the persons acting under its authority who have access to the personal data in question. Such persons must be required to give an undertaking of confidentiality;
- to appoint system administrators in accordance with the indications of the relevant Provision of the Italian Data Protection Authority, providing the necessary instructions;
- to inform the Controller, as soon as it becomes aware of them, of any personal data breaches, even

suspected ones, or of security incidents that may give rise to such breaches;
- to make available to the Controller all the information necessary to demonstrate compliance with the obligations set out in this article and to allow for and contribute to audits, including inspections, conducted by the Controller, by another party appointed by the Controller or by the supervisory authority;
- to assist the Controller in fulfilling the Controller's obligation to respond to requests for the exercise of the data subject's rights;
- where requested, to cooperate with the Controller in carrying out the impact assessment of the processing, examining the need for any prior consultation of the supervisory authority;
- to adopt technical and organisational measures to ensure a level of security appropriate to the risk, taking particular account of the risks that may arise from the destruction, loss, alteration or unauthorised disclosure of, or access to, the personal data processed, whether accidental or unlawful. The security measures adopted are detailed for each service in the following article.

3. Obligations of the Customer

The Customer, as Controller, is responsible for:
- verifying the lawfulness of the processing, identifying its legal basis;
- providing the privacy notice to the data subjects;
- requesting consent, if required;
- if necessary, carrying out the impact assessment;
- assessing the adequacy of the measures adopted to protect the data and described in Article 6 below for each service. The Customer may contact Qcom for any additions, changes and implementations;
- verifying the lawfulness of the processing of data in the context of any promotional campaigns and web marketing activities entrusted to Qcom. In particular, the Customer must assess the consistency of its privacy policy with the activities requested from Qcom. This verification and, where appropriate, the preparation of an adequate privacy policy may be carried out by Qcom under a specific agreement.

4. Other processors

In order to carry out processing on behalf of the Controller, the Processor may engage other processors. In any case, the Processor must impose on the sub-processor it uses the same data protection obligations as those set out in this deed, providing in particular sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing meets the requirements of the Regulation. Where the other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the other processor's obligations. The Controller, if it so requests, shall be kept informed of the engagement of other processors.

5. Duration

Qcom acts as Processor for as long as the services are provided to the Customer.

6. Security measures

To protect the data, Qcom, as Processor, adopts the following measures, described for each service.

CLOUD VIRTUAL SERVER

- IP/port-level access control and restriction: our perimeter firewall blocks all access to the machines for all services not explicitly requested by the customer;
- periodic snapshots: periodically, several times a day, a snapshot of the server is taken and kept, read-only, for a time sufficient to remedy any data loss due to software problems and/or malware;
- asynchronous replication on redundant hardware: the snapshots are copied to a second site, on redundant hardware, so as to have a restore point in the event of a disaster at the production site;
- data storage within national territory: all data are stored on equipment owned by Qcom located within national territory;
- malware detection: constant monitoring of the machines' activities so as to intercept any anomalies;
- periodic operating system updates: all systems are updated periodically;
- daily backup: if provided for in the contractual plan, a backup of the data hosted on the machine is made daily;

EMAIL

- use of secure protocols: all our servers are configured to use encrypted communications, according to the most secure standards. Obsolete protocols (SSL2/SSL3) are disabled;
- encrypted credential exchange: if the client, owing to a shortcoming of its own, fails to establish an encrypted protocol (TLS), authentication protocols that do not provide for an encrypted exchange of the password (LOGIN/PLAIN) are automatically disabled. In this way the user can be certain that credentials are exchanged securely;
- antivirus: all emails are checked by at least one antivirus system; incoming emails, in particular, are checked by three different antivirus engines;
- sandboxing: where provided for in the contractual plan, incoming emails are processed by a powerful anti-malware engine that analyses the behaviour of attached documents in special sandboxes, so as to recognise malware not by its signature but by its behaviour, according to the most modern techniques available;
- antispam: all emails in transit are checked by at least one antispam system; incoming emails are checked in cascade by two separate antispam systems, to minimise attacks carried out using social engineering techniques;
- snapshots and asynchronous replication: periodically, several times a day, a snapshot of the stored emails is taken and kept, read-only, for one week. It is also replicated to a second site, on redundant hardware, so as to have a restore point in the event of a disaster at the production site.

MANAGED HOSTING

- use of secure protocols: all our servers are configured to use encrypted communications, according to the most secure standards. Obsolete protocols (SSL2/SSL3) are disabled. At the customer's request, a free https x509 certificate can be activated or, where provided for in the contract, a paid certificate can be uploaded;
- isolation: each site is isolated and protected from the other sites hosted on the web farm: if a neighbouring site is attacked, the attack cannot affect the others;
- daily backup: an indexed backup of the site content and of the database is made every day; these backups are kept, with decreasing granularity, for up to six months;
- snapshots and asynchronous replication: periodically, several times a day, a snapshot of the sites' code and databases is taken and kept, read-only, for one week. It is also replicated to a second site, on redundant hardware, so as to have a restore point in the event of a disaster at the production site;

- abuse control: anomalous activity by the code uploaded by the customer is identified and handled by Qcom staff;
- data storage within national territory: all data are stored on equipment owned by Qcom located within national territory.

CLOUD GARAGE

- use of secure protocols: all our servers are configured to use encrypted communications, according to the most secure standards. Obsolete protocols (SSL2/SSL3) are disabled;
- firewall protection: the service is always sold in combination with a firewall that regulates access, reducing the risks;
- isolation: each customer space is isolated and protected from other sites; uploaded data are invisible to third parties;
- data storage within national territory: all data are stored on equipment owned by Qcom located within national territory.

CLOUD GARAGE

- use of secure protocols: all our servers are configured to use encrypted communications, according to the most secure standards. Obsolete protocols (SSL2/SSL3) are disabled;
- constantly updated software: both the server-side software and the installed agents are automatically and constantly updated to guarantee maximum security;
- guaranteed backup: the customer is periodically informed of the progress of backups by summary emails that clearly show what has been saved;
- maximum reliability: the data are stored on redundant hardware, to guarantee their preservation even in the event of hardware failures;
- maximum security: at the customer's request, the data can be made inaccessible even to Qcom technicians, by protecting them with an additional password;
- data storage within national territory: all data are stored on equipment owned by Qcom located within national territory.

CLOUD SECURE BOX AND SECURE BOX

- constantly updated software: both the server-side software and the installed agents are automatically and constantly updated to guarantee maximum security;
- confidentiality: the aggregated traffic data stored on the devices, used to generate the statistics and reports contracted by the customer, are the property of the customer and are not used by Qcom for other purposes or resold to third parties;
- security: the aggregated traffic data stored on the devices make it possible to identify any vulnerabilities, critical issues, anomalies or attacks, providing the customer with the appropriate tools to remedy them;
- storage within national territory: all the devices will be located in datacenters situated within national territory.

VIRTUAL PBX PHONE SYSTEM

- redundant infrastructure: the devices that carry the telephone traffic are redundant to guarantee service continuity;
- confidentiality: the audio stream passes through dedicated devices owned by Qcom and is not stored;
- compliance: traffic data are stored and retained as required by the relevant laws;
- data storage within national territory: all the data and devices involved are owned by Qcom and located within national territory.

NEWSLETTER

- use of secure protocols: all our servers are configured to use encrypted communications, according to the most secure standards. Obsolete protocols (SSL2/SSL3) are disabled;
- encrypted credential exchange: if the client, owing to a shortcoming of its own, fails to establish an encrypted protocol (TLS), authentication protocols that do not provide for an encrypted exchange of the password (LOGIN/PLAIN) are automatically disabled. In this way the user can be certain that credentials are exchanged securely;
- antivirus: all emails are checked by at least one antivirus system; incoming emails, in particular, are checked by three different antivirus engines;
- sandboxing: incoming emails are processed by a powerful anti-malware engine that analyses the behaviour of attached documents in special sandboxes, so as to recognise malware not by its signature but by its behaviour, according to the most modern techniques available;
- antispam: all emails in transit are checked by at least one antispam system; incoming emails are checked in cascade by two separate antispam systems, to minimise attacks carried out using social engineering techniques;
- dedicated firewall that enforces access policies, limits and regulates data flows to prevent abuse and keeps track of the connections established;
- The databases and file systems of the information systems are backed up (at least) daily. The data are stored on a disk system separate from the production one and have a retention of up to six (6) months, with decreasing granularity;
- Users' Windows PCs are configured to synchronise the content of the desktop and documents with the file server; this server is configured to perform two backups a day.

Qcom provides the service through Coriweb srl, which has been duly appointed and bound to comply with similar security measures, including if it in turn uses sub-processors.

ONLINE ADVERTISING CAMPAIGNS AND WEB MARKETING

- use of secure protocols: all our servers are configured to use encrypted communications, according to the most secure standards. Obsolete protocols (SSL2/SSL3) are disabled;
- encrypted credential exchange: if the client, owing to a shortcoming of its own, fails to establish an encrypted protocol (TLS), authentication protocols that do not provide for an encrypted exchange of the password (LOGIN/PLAIN) are automatically disabled. In this way the user can be certain that credentials are exchanged securely;
- antivirus: all emails are checked by at least one antivirus system; incoming emails, in particular, are checked by three different antivirus engines;
- sandboxing: incoming emails are processed by a powerful anti-malware engine that analyses the behaviour of attached documents in special sandboxes, so as to recognise malware not by

its signature but by its behaviour, according to the most modern techniques available;

- antispam: all emails in transit are checked by at least one antispam system; incoming emails are checked in cascade by two separate antispam systems, to minimise attacks carried out using social engineering techniques;
- dedicated firewall that enforces access policies, limits and regulates data flows to prevent abuse and keeps track of the connections established;
- The databases and file systems of the information systems are backed up (at least) daily. The data are stored on a disk system separate from the production one and have a retention of up to six (6) months, with decreasing granularity;
- Users' Windows PCs are configured to synchronise the content of the desktop and documents with the file server; this server is configured to perform two backups a day.

This document is an English translation of the original Italian document and is provided for ease of reference. The translation may contain errors, omissions or inaccuracies. In the event of any discrepancy or inconsistency between this translation and the Italian original, the Italian original shall prevail to the extent permitted by applicable law.