Accordo ai sensi dell'articolo 28 del Regolamento 2016/679/UE tra il Cliente (di seguito definito "Titolare") e Qcom SpA (di seguito definito "Responsabile")

1. Servizi per i quali Qcom opera come Responsabile del trattamento

Per i seguenti servizi che richiedono il trattamento di dati personali per conto del Cliente, Qcom opera come Responsabile del trattamento:

Servizio	Trattamenti effettuati per conto del Cliente	Dati personali trattati
Cloud Virtual Server	Trattamenti (principalmente la conservazione) di eventuali dati personali che risiedano sul virtual server	Non noti
Posta elettronica	Trattamenti (principalmente la conservazione) di eventuali dati personali che risiedano sul server di posta	Non noti
Hosting gestito	Trattamenti (principalmente la conservazione) di eventuali dati personali che risiedano sul sito del cliente in hosting	Non noti
Cloud Garage	Trattamenti (principalmente la conservazione) di eventuali dati personali che risiedano nello spazio cloud a disposizione	Non noti
Cloud Backup	Trattamenti (principalmente conservazione e copia) di eventuali dati personali che risiedano nello spazio cloud a disposizione	Non noti
Cloud secure box e secure box	Trattamenti (principalmente conservazione e copia) di eventuali dati personali che risiedano nello spazio cloud a disposizione	Non noti
Centralino virtuale PBX	Trattamenti (principalmente la conservazione) dei dati relativi alle chiamate in entrata e in uscita	Dati di traffico telefonico
Newsletter	Trattamenti (principalmente invio e conservazione) di newsletter e comunicazioni promozionali	Indirizzi mail dei destinatari forniti dal Cliente
Campagne pubblicitarie online e webmarketing	Trattamenti (principalmente la raccolta di contatti e l'invio di comunicazioni promozionali) effettuati anche come amministratore del profilo "social" del Cliente	Indirizzi mail, numeri telefonici, contatti su piattaforme acquisiti per conto del Cliente o forniti da quest'ultimo

2. Obblighi di Qcom

Qcom, quale Responsabile del trattamento si attiene a quanto qui di seguito riportato:

- non comunicare a terzi in alcun modo e non utilizzare per altri fini i dati personali e comunque mantenere la più completa riservatezza sui dati trattati e sulle tipologie di trattamento effettuate. Tali obblighi sono da considerarsi pienamente vigenti anche nel caso di cessazione del presente rapporto contrattuale;
- non trasferire in alcun modo i dati in un paese extra UE e nel caso ciò si rivelasse necessario, informare il Titolare delle soluzioni adottate in adempimento alle prescrizioni normative;
- istruire adeguatamente le persone che operano sotto la sua autorità avendo accesso ai dati personali in questione. A tali persone è essere richiesto un impegno di riservatezza;
- nominare gli amministratori di sistema secondo le indicazioni del Provvedimento relativo del Garante fornendo le necessarie istruzioni;
- comunicare al Titolare, non appena ne abbia avuto conoscenza, eventuali violazioni dei dati personali anche

sospette o incidenti di sicurezza da cui possano derivare tali violazioni;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consentire e contribuire alle attività di vigilanza, comprese le ispezioni, realizzate dal Titolare, da un altro soggetto da questi incaricato o dall'Autorità di controllo;
- assistere il Titolare al fine di soddisfare l'obbligo di quest'ultimo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- qualora gli sia richiesto, collaborare con il Titolare a effettuare la valutazione di impatto dei trattamenti vagliando la necessità dell'eventuale consultazione preventiva dell'Autorità di controllo;
- adottare misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, considerando in special modo i rischi che possono derivare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati. Le misure di sicurezza adottate sono dettagliate per ciascun servizio al seguente articolo.

3. Obblighi del Cliente

Al Cliente, quale Titolare del trattamento, spetta:
- verificare la legittimità del trattamento, individuandone la base giuridica;
- fornire l'informativa agli interessati;
- richiedere il consenso, se richiesto;
- se necessario, effettuare la valutazione di impatto;
- valutare l'adeguatezza delle misure adottate a protezione dei dati e descritte al seguente articolo 6 per ciascun servizio. Potrà rivolgersi a Qcom per eventuali integrazioni, modifiche e implementazioni;
- verificare la legittimità del trattamento dei dati nell'ambito delle campagne promozionali e delle attività di web marketing che fossero affidate a Qcom. In particolare, dovrà valutare la coerenza della sua privacy policy rispetto alle attività richieste a Qcom. Tale verifica e l'eventuale predisposizione di una privacy policy adeguata potranno essere effettuate da Qcom a seguito di specifico accordo.

4. Altri responsabili

Il Responsabile, per effettuare i trattamenti per conto del Titolare, può ricorrere ad altri responsabili. In ogni caso, il Responsabile dovrà imporre al sub-responsabile di cui si serve gli stessi obblighi in materia di protezione dei dati stabiliti nel presente atto, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile. Il Titolare, se richiesto, è aggiornato in merito al ricorso ad altri responsabili.

5. Durata

Qcom opera come Responsabile per tutto il tempo in cui i servizi sono erogati al Cliente.

6. Misure di sicurezza

A protezione dei dati Qcom, quale Responsabile del trattamento, adotta le seguenti misure, descritte per ciascun servizio.

CLOUD VIRTUAL SERVER

- controllo e limitazione accesso a livello di IP/porta: il nostro firewall perimetrale blocca ogni accesso alle macchine per tutti i servizi non esplicitamente richiesti dal cliente;
- snapshot periodiche: con cadenza periodica, più volte al giorno, il server è fotografato e lo snapshot conservato, in sola lettura per un tempo sufficiente a rimediare eventuali perdite di dati dovuti a problemi software e/o malware;
- replica asincrona su hardware ridondato: gli snapshot sono copiati su un secondo sito, su hardware ridondante, in modo da poter avere un punto di ripristino in caso di catastrofe sul sito di produzione;
- conservazione dei dati sul territorio nazionale: tutti i dati sono conservati su apparati di proprietà di Qcom ubicati all'interno del territorio nazionale;
- rilevamento malware: monitoraggio costante delle attività delle macchine in modo da intercettare eventuali anomalie;
- aggiornamento periodico del sistema operativo: tutti i sistemi sono periodicamente aggiornati;
- backup giornaliero: se previsto dal piano contrattuale, viene effettuato giornalmente un backup dei dati ospitati sulla macchina;

POSTA ELETTRONICA

- utilizzo di protocolli sicuri: tutti i nostri server sono configurati per utilizzare comunicazioni cifrate, secondo gli standard più sicuri. I protocolli obsoleti (SSL2/SSL3) sono disattivati;
- scambio credenziali cifrate: qualora il client, a causa di una propria mancanza, non riesca a stabilire un protocollo cifrato (TLS), sono disattivati automaticamente i protocolli di autenticazione che non prevedono uno scambio cifrato della password (LOGIN/PLAIN). In questo modo l'utente è certo che lo scambio delle credenziali avviene in modo sicuro;
- antivirus: tutte le e-mail sono controllate da almeno un sistema antivirus; le mail in ingresso, in particolare, sono controllate da tre diversi motori antivirus;
- sandboxing: qualora sia previsto dal piano contrattuale, le mail in ingresso sono processate da un potente motore anti-malware che analizza il comportamento dei documenti allegati in particolari sandbox, in modo da riconoscere il malware non tramite firma ma tramite il comportamento, secondo le più moderne tecniche esistenti;
- antispam: tutte le e-mail in transito sono controllate da almeno un sistema antispam; quelle in ingresso sono controllate in cascata da due sistemi antispam distinti, per ridurre al minimo gli attacchi portati con tecniche di ingegneria sociale;
- snapshot e replica asincrona: con cadenza periodica, più volte al giorno, le e-mail in giacenza sono fotografate e lo snapshot conservato, in sola lettura, per una settimana. Viene inoltre replicato su un secondo sito, su hardware ridondante, in modo da poter avere un punto di ripristino in caso di catastrofe sul sito di produzione.

HOSTING GESTITO

- utilizzo di protocolli sicuri: tutti i nostri server sono configurati per utilizzare comunicazioni cifrate, secondo gli standard più sicuri. I protocolli obsoleti (SSL2/SSL3) sono disattivati. Su richiesta del cliente, può essere attivato un certificato https x509 gratuito o, qualora previsto dal contratto, caricato un certificato a pagamento;
- isolamento: ogni sito è isolato e protetto dagli altri siti caricati sulla web farm: in caso di attacco ad un sito vicino, questo non può ripercuotersi sugli altri;
- backup giornaliero: ogni giorno viene effettuato un backup indicizzato del contenuto del sito e del database; tali backup sono conservati, con granularità decrescente, fino a sei mesi;
- snapshot e replica asincrona: con cadenza periodica, più volte al giorno, il codice ed i database dei siti sono fotografati e lo snapshot conservato, in sola lettura, per una settimana. Viene inoltre replicato su un secondo sito, su hardware ridondante, in modo da poter avere un punto di ripristino in caso di catastrofe sul sito di produzione;
- controllo degli abusi: attività anomale da parte del codice caricato dal cliente vengono individuate e gestite dal personale Qcom;
- conservazione dei dati sul territorio nazionale: tutti i dati sono conservati su apparati di proprietà di Qcom ubicati all'interno del territorio nazionale.

CLOUD GARAGE

- utilizzo di protocolli sicuri: tutti i nostri server sono configurati per utilizzare comunicazioni cifrate, secondo gli standard più sicuri. I protocolli obsoleti (SSL2/SSL3) sono disattivati;
- protezione tramite firewall: il servizio è sempre venduto in associazione con un firewall che regola gli accessi, abbattendo i rischi;
- isolamento: ogni spazio fornito al cliente è isolato e protetto dagli altri siti; i dati caricati sono invisibili a terzi;
- conservazione dei dati sul territorio nazionale: tutti i dati sono conservati su apparati di proprietà di Qcom ubicati all'interno del territorio nazionale.

CLOUD GARAGE

- utilizzo di protocolli sicuri: tutti i nostri server sono configurati per utilizzare comunicazioni cifrate, secondo gli standard più sicuri. I protocolli obsoleti (SSL2/SSL3) sono disattivati;
- software costantemente aggiornato: sia il software lato server, che gli agent installati sono automaticamente e costantemente aggiornati per garantire la massima sicurezza;
- backup garantito: il cliente è informato periodicamente sull'andamento dei backup tramite mail di riepilogo che mostrano chiaramente cosa è stato salvato;
- massima affidabilità: i dati sono conservati su un hardware ridondante, per garantire la conservazione anche in caso di rotture hardware;
- massima sicurezza: su richiesta del cliente è possibile rendere inaccessibili i dati anche ai tecnici Qcom, proteggendoli tramite una password aggiuntiva;
- conservazione dei dati sul territorio nazionale: tutti i dati sono conservati su apparati di proprietà di Qcom ubicati all'interno del territorio nazionale.

CLOUD SECURE BOX E SECURE BOX

- software costantemente aggiornato: sia il software lato server, che gli agent installati sono automaticamente e costantemente aggiornati per garantire la massima sicurezza;
- riservatezza: i dati aggregati di traffico memorizzati sugli apparati sono utilizzati per generare le statistiche ed i report contrattualizzati dal cliente sono di proprietà del cliente e non vengono utilizzati da Qcom per fini differenti né rivenduti a terzi;
- sicurezza: i dati aggregati di traffico memorizzati sugli apparati consentono di individuare eventuali vulnerabilità, criticità, anomalie o attacchi, fornendo al cliente gli strumenti adeguati per porvi rimedio;
- conservazione all'interno del territorio nazionale: tutti gli apparati saranno collocati in datacenter ubicati all'interno del territorio nazionale.

CENTRALINO VIRTUALE PBX

- infrastruttura ridondante: gli apparati che erogano il traffico telefonico sono ridondati per garantire continuità al servizio;
- riservatezza: il flusso audio transita su apparati dedicati di proprietà Qcom e non viene memorizzato;
- conformità: i dati di traffico sono memorizzati e conservati come dettato dalle norme di legge in materia;
- conservazione dei dati sul territorio nazionale: tutti i dati e gli apparati coinvolti sono di proprietà di Qcom e ubicati all'interno del territorio nazionale.

NEWSLETTER

- utilizzo di protocolli sicuri: tutti i nostri server sono configurati per utilizzare comunicazioni cifrate, secondo gli standard più sicuri. I protocolli obsoleti (SSL2/SSL3) sono disattivati;
- scambio credenziali cifrate: qualora il client, a causa di una propria mancanza, non riesca a stabilire un protocollo cifrato (TLS), sono disattivati automaticamente i protocolli di autenticazione che non prevedono uno scambio cifrato della password (LOGIN/PLAIN). In questo modo l'utente è certo che lo scambio delle credenziali avviene in modo sicuro;
- antivirus: tutte le e-mail sono controllate da almeno un sistema antivirus; le mail in ingresso, in particolare, sono controllate da tre diversi motori antivirus;
- sandboxing: le mail in ingresso sono processate da un potente motore anti-malware che analizza il comportamento dei documenti allegati in particolari sandbox, in modo da riconoscere il malware non tramite firma ma tramite il comportamento, secondo le più moderne tecniche esistenti;
- antispam: tutte le e-mail in transito sono controllate da almeno un sistema antispam; quelle in ingresso sono controllate in cascata da due sistemi antispam distinti, per ridurre al minimo gli attacchi portati con tecniche di ingegneria sociale;
- firewall dedicato che impone le policy di accesso, limita e regola i flussi di dati per evitare abusi e tiene traccia delle connessioni instaurate;
- I database e i filesystem dei sistemi informativi sono sottoposti a backup (almeno) quotidiano. I dati sono memorizzati su un sistema dischi separato da quello di produzione e hanno una retention che arriva a sei (6) mesi, con granularità decrescente;
- I PC windows degli utenti sono configurati per sincronizzare con il file server il contenuto del desktop e dei documenti; tale server è configurato per effettuare due backup al giorno.

Qcom offre il servizio attraverso Coriweb srl che è stata adeguatamente nominata e vincolata al rispetto di analoghe misure di sicurezza anche nel caso utilizzasse a sua volta sub-responsabili.

CAMPAGNE PUBBLICITARIE ONLINE E WEB MARKETING

- utilizzo di protocolli sicuri: tutti i nostri server sono configurati per utilizzare comunicazioni cifrate, secondo gli standard più sicuri. I protocolli obsoleti (SSL2/SSL3) sono disattivati;
- scambio credenziali cifrate: qualora il client, a causa di una propria mancanza, non riesca a stabilire un protocollo cifrato (TLS), sono disattivati automaticamente i protocolli di autenticazione che non prevedono uno scambio cifrato della password (LOGIN/PLAIN). In questo modo l'utente è certo che lo scambio delle credenziali avviene in modo sicuro;
- antivirus: tutte le e-mail sono controllate da almeno un sistema antivirus; le mail in ingresso, in particolare, sono controllate da tre diversi motori antivirus;
- sandboxing: le mail in ingresso sono processate da un potente motore anti-malware che analizza il comportamento dei documenti allegati in particolari sandbox, in modo da riconoscere il malware non tramite

firma ma tramite il comportamento, secondo le più moderne tecniche esistenti;
- antispam: tutte le e-mail in transito sono controllate da almeno un sistema antispam; quelle in ingresso sono controllate in cascata da due sistemi antispam distinti, per ridurre al minimo gli attacchi portati con tecniche di ingegneria sociale;
- firewall dedicato che impone le policy di accesso, limita e regola i flussi di dati per evitare abusi e tiene traccia delle connessioni instaurate;
- I database e i filesystem dei sistemi informativi sono sottoposti a backup (almeno) quotidiano. I dati sono memorizzati su un sistema dischi separato da quello di produzione e hanno una retention che arriva a sei (6) mesi, con granularità decrescente;
- I PC windows degli utenti sono configurati per sincronizzare con il file server il contenuto del desktop e dei documenti; tale server è configurato per effettuare due backup al giorno.