# REGISTRO DEI TRATTAMENTI E MISURE DI SICUREZZA DEL SERVIZO SIMPLE BOOKING E DEI PRODOTTI COLLEGATI IN RELAZIONE ALLE PRESCRIZIONI DEL GDPR

| RESPONSABILE DEL TRATTAMENTO | | | | | |
|---|---|---|---|---|---|
| **Denominazione** | QNT S.r.l. Socio Unico | | | | |
| **Partita Iva** | IT02333620488 | | | | |
| **Indirizzo** | Via Lucca 52 | | | | |
| **Città** | Firenze | **Cap** | 50142 | **PV** | FI |
| **Legale Rappresentante** | Sergio Farinelli | | | | |

| STRUTTURA ORGANIZZATIVA | | | |
|---|---|---|---|
| **Divisione** | Simple Booking | Responsabile Divisione | Sergio Farinelli |

| INCARICATI DEL TRATTAMENTO |
|---|
| Addetti analisi, sviluppo, controllo qualità, help desk, sistemisti |

| DATI DI CONTATTO | | | |
|---|---|---|---|
| **Referente Aziendale** | Sergio Farinelli | privacy@simplebooking.travel | 055705718 |

| DESCRIZIONE |
|---|
| Simple Booking ed iRev Channel Manager gestiscono i dati anagrafici ed in certi casi quelli di pagamento di clienti finali che effettuano richieste e prenotazioni nella piattaforma e degli incaricati dal Titolare che accedono al BackOffice per gestire le pratiche. |

| FINALITA' DEL TRATTAMENTO |
|---|

Gestione dei dati personali di clienti finali utilizzati per consentire al Titolare di fornire i propri servizi e per le seguenti finalità:

- Ricezione prenotazioni
- Ricezione richieste di disponibilità
- Invio di preventivi
- Acquisizione pagamenti
- Contattare l'Utente
- Analisi Statistica
- Assistenza tecnica

## CATEGORIA INTERESSATI

1) Utenti finali che hanno effettuato prenotazioni (dirette o tramite uno dei canali connessi: OTA, GDS, Metasearch )
2) Utenti che hanno fornito i propri dati per inviare richieste all'hotel (disponibilità ,preventivi)
3) Utenti applicativi creati dal titolare per accedere al backoffice Simple Booking

## CATEGORIE DI DATI PERSONALI

Nominativo ed email degli utenti che hanno prenotato o inviato una richiesta.
Altri dati anagrafici degli utenti (indirizzo e recapiti telefonici) se richiesti dall'hotel
Dati di pagamento per le prenotazioni (solo per alcune)

Nominativo ed email degli utenti applicativi creati dal Titolare per accedere al BackOffice Simple Booking

I prodotti che usano la base dati comune sono:
Simple Booking
iRev Channel Manager

## CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Sistemi terzi (ad es. PMS, channel managers, CRM di terze parti) autorizzati dal Titolare e connessi via API al sistema Simple Booking.
L'autorizzazione alla trasmissione dei dati viene fornita in forma scritta dal titolare stesso.
I dati potranno essere comunicati anche alle autorità preposte qualora per legge ci sia l'obbligo di comunicazione.

## TRASFERIMENTO DATI ALL'ESTERO

Si, su richiesta scritta del titolare è possibile inviare le informazioni relative alle prenotazioni comprensive dei dati personali del prenotante a sistemi terzi quali ad es. PMS, channel managers, CRM, ecc.

Tali sistemi potrebbero risiedere anche all'estero, sia perché il titolare ha la sede all'estero dove è istallato l'applicativo PMS, sia perché può utilizzare un sistema terzo in Cloud i cui server potrebbero risiedere all'estero, potenzialmente anche fuori dalla Comunità Europea.

E' responsabilità del Titolare verificare la compliance del sistema terzo a cui ci ha autorizzato a trasferire i dati, nei confronti delle proprie politiche sulla privacy e di quanto previsto dalle normative vigenti.

| VERIFICA DELLE SICUREZZE A LIVELLO APPLICATIVO |
|---|
| Il Titolare potrà verificare le sicurezze impostate al livello di ogni singolo account utente creato dal titolare stesso visualizzando l'apposita sezione all'interno del BackOffice.<br>Da tale sezione il Titolare potrà verificare e modificare le autorizzazioni e le modalità di autenticazione associate al singolo account utente oltre che disattivare l'account stesso.<br>Tutti i dati vengono trasmessi esclusivamente in forma cifrata utilizzando protocolli sicuri. |

| TERMINI PER LA CANCELLAZIONE DEI DATI |
|---|
| I dati conservati in SimpleBooking ed iRev Channel manager saranno conservati per tutta la durata del contratto di prenotazione e per il tempo di conservazione indicato dal titolare all'interno della piattaforma. Saranno anche conservati su supporti di backup per tutta la durata del contratto di prenotazione e per default per i 12 mesi successivi alla sua cessazione.<br>Il Titolare ha la possibilità, attraverso le funzioni applicative di lanciare procedure di richiesta di anonimizzazione dei dati personali degli utenti salvati nel db oppure di impostare la scadenza entro la quale, successivamente al termine del contratto di prenotazione, ne sarà richiesta automaticamente l'anonimizzazione. |

## DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

### 1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

- Gestione credenziali di accesso
- User name: l'accesso al BackOffice avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema c'è una credenziale amministrativa che viene consegnata al titolare e da questo utilizzabile sono in circostanze eccezionali. Il titolare deve predisporre una procedura organizzativa affinché tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione.
- Password: le regole di complessità della password rispettano quelle imposte dalla normativa vigente e da quanto prescritto per i sistemi PCI DSS.
- Disattivazione/disabilitazione credenziali
- Tutti gli utenti devono essere abilitati a livello di IP per accedere all'area di BackOffice
- E' possibile implementare una two-factor authentication attraverso un sistema di TOTP in aggiunta o in sostituzione al controllo dell'IP

- Minimizzazione
- Profili di autorizzazione: il Titolare può configurare l'accesso alle varie funzioni del software e ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti.
- Identificazione di chi ha trattato i dati
- Strumenti di log: sono presenti i log della procedura con cui sono registrati gli accessi alla procedura stessa e alle singole funzioni che la compongono con il tipo di operazione eseguita. I log sono conservati nel sistema per almeno 12 mesi.
- Tutti coloro che accedono al BackOffice dovranno aver ricevuto dal titolare il proprio account nominale al quale sono state assegnate le autorizzazioni minime necessarie per operare e che potrà essere attivato e disattivato dal Titolare in funzione della necessità.
- Tecniche di crittografia
- Crittografia della base dati: La crittografia della base dati avviene sui dati di pagamento e su quelle di autenticazione degli utenti.
- Privacy by default
- Attivazione profilo utente: gli utenti nel BackOffice sono attivati secondo una logica di non assegnare alcun profilo autorizzativo sui dati trattati. Sarà il Titolare in autonomia a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale.
- Diritti degli interessati
- Diritti degli interessati: per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che farà le opportune valutazioni. Qualora il Titolare decida che i dati debbano essere cancellati potrà agire direttamente sul BackOffice, effettuando la richiesta di anonimizzazione dall'anagrafica all'interno di ogni prenotazione. Nei singoli applicativi saranno presenti quindi solo informazioni anonime non riconducibili neppure indirettamente ad alcun interessato.
- Per garantire il diritto dell'interessato di avere informazione su quali dati tratta il Titolare e alla portabilità dei suoi dati, all'interno del BackOffice c'è la possibilità di fare delle estrazioni HTML sia della parte anagrafica che di ogni parte applicativa che riguardano quell'interessato. Con l'HTML il Titolare potrà trasmettere i dati all'interessato che potrà trattarli per le sue finalità. Qualora l'HTML non fosse sufficiente l'esportazione potrà avvenire in XML o CSV.

*Queste misure di sicurezza devono essere correttamente impostate da parte del Titolare.*

## 1. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

### ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

### ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email i tecnici QNT inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.

### ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO TEAM VIEWER

Questa modalità di collegamento sugli strumenti dei Titolari garantisce la privacy in quanto:

- Il collegamento è sempre richiesto ed autorizzato dal Titolare
- Le credenziali di accesso sono sempre individuali
- Il Titolare fa accedere i tecnici QNT ad un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza
- Il Titolare può disconnettere il tecnico quando desidera

## 2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE

| CODICE | CLASSE DELLA MISURA | LIVELLO DI APPLICAZIONE |
|---|---|---|
| M1 | Sicurezza locali e apparati | Il datacenter dove sono ubicate le aree tecniche di competenza QNT è protetto da misure che controllano l'accesso fisico ai locali. |
| M2 | Autenticazione | I sistemi ed i servizi QNT sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate agli incaricati. |
| M3 | Sistema di autorizzazione | L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti a livello del sistema operativo della piattaforma che ospita l'applicazione e a livello applicativo. |
| M4 | Controllo integrità dei dati | Sono attivi servizi di controllo per presenza di virus sia nei file systems locali dei singoli PC che nei file system condivisi, oltre che sui messaggi di posta elettronica. |
| M5 | Backup e Ripristino dei dati | Sono in atto politiche di backup per i dati. |
| M6 | Gestione delle politiche di sicurezza | Sono predisposte delle Policy IT indirizzate alla sicurezza. |
| M7 | Formazione degli incaricati | E' previsto un piano di formazione e di aggiornamento per gli incaricati di QNT. |
| M8 | Supporti rimovibili | Sono disposte regole per la gestione di supporti removibili in presenza di dati sensibili. |

| | | |
|---|---|---|
| M9 | Procedure automatiche di cancellazione dati utenti interni | Ci sono regole di cancellazione dei dati in relazione alle diverse attività svolte |

Classificazione e scheda dettagliata delle Misure di sicurezza adottate

| CLASSE MISURA | MISURA | DESCRIZIONE SINTETICA |
|---|---|---|
| M1. | 1.1 Sistemi di allarme anti intrusione | È previsto un sistema di allarme contro le intrusioni. In caso di intrusione in SERVER FARM il sistema di allarme provvede ad avvisare automaticamente il servizio di guardia giurata notturno |
| | 1.2 Accesso alle postazioni di lavoro | L'accesso viene consentito tramite identificazione effettuata tramite credenziali assegnate ad ogni dipendente. Le autorizzazioni di accesso sono fornite dagli amministratori di sistema che abilita in funzione della mansione svolta o delle esigenze segnalate. |
| | 1.3 Controllo Accessi Aree Riservate | Per i locali a più alto rischio quale il CED di sede QNT e la SERVER FARM, l'accesso agli stessi è consentito solo a personale autorizzato. |
| | 1.4 Prevenzione incendi | I locali della SERVER FARM sono dotati di impianti automatici di rivelazione fumo. I locali tecnici prevedono un impianto per lo spegnimento degli incendi. Sono applicate le misure di sicurezza previste dal Dlgs 81/2008. |
| | 1.5 Dislocazione degli apparati attivi e dei server di rete | Tutti gli apparati attivi ed i server di rete sono dislocati in locali tecnici ad accesso controllato. |
| | 1.6 Registrazione accessi agli uffici | Data ed ora di ingresso ed uscita del personale vengono registrati tramite l'ausilio di apparecchi di rilevazione presenze. |
| | 1.7 Videosorveglianza | Presso la SERVER FARM sono attivi sistemi di videosorveglianza e le relative modalità di gestione sono descritte in apposite procedure. |

| | | |
|---|---|---|
| M2. | 2.1 Adozione di procedure di gestione delle credenziali di Autenticazione: USERNAME | Tutti i lavoratori sono identificati nel sistema informativo attraverso una user name assegnata in modo univoco agli stessi.<br>La User name non sarà associata ad altri lavoratori neppure in tempi diversi.<br>Qualora vi sia omonimia la user verrà creata in modo da creare sempre univocità e riconoscibilità di esecuzione di trattamenti di dati personali.<br>Le username si suddividono in username per accesso ad ambienti di lavoro e username per accesso alle applicazioni funzionali.<br>Ogni sistema ha la propria gestione e memorizzazione della username. |
| | 2.2 Adozione di procedure di gestione delle credenziali di Autenticazione: PASSWORD | L'accesso ad ogni ambiente o strumento elettronico avviene attraverso credenziali di autenticazione.<br>La password al primo accesso viene impostata dall'ufficio tecnico che configura inizialmente l'ambiente di lavoro di ogni singolo incaricato. A seconda del sistema vengono seguite le seguenti regole:<br>- per l'accesso ai sistemi operativi di sede viene impostato per il primo accesso una password che l'utente è obbligato a cambiare la password al primo accesso.<br>- per l'accesso agli altri sistemi viene impostato per il primo accesso una password che l'utente è obbligato a cambiare.<br>Ogni utente che inizia un trattamento di dati personali viene edotto sull'importanza che la componente riservata della credenziale di autenticazione non venga divulgata ad altri operatori.<br>Inoltre l'incaricato viene formato sulle regole minime di composizione della password<br>L'incaricato viene inoltre edotto sulla necessità di modifica delle password ogni 3 mesi.<br>Gli strumenti utilizzati per i trattamenti in alcuni casi non gestiscono in autonomia il cambio password, né effettuano controlli sulla ripetitività delle stesse password nel tempo.<br>Quindi tali adempimenti sono a carico dello stesso utente che assume tale onere con la sottoscrizione della lettera di incarico.<br>Le password di tutti i sistemi elettronici quando vengono digitate sono in formato inintelligibile. |
| | 2.3 Uso esclusivo delle credenziali di autenticazione. | Ogni credenziale di autenticazione (username e password) viene assegnata ad un unico operatore che la utilizzerà in modo esclusivo. |

| | | |
|---|---|---|
| | 2.4 Disattivazione delle credenziali di autenticazione per mancato utilizzo (+ 6 mesi) o perdita qualità | Nel caso in cui un incaricato dovesse perdere la qualità per la quale gli erano state assegnate le credenziali di autenticazione (ad esempio cessazione dell'attività in azienda, oppure cambio di mansione di ruolo, etc). le credenziali al medesimo riferite saranno disattivate e non verranno più utilizzate. |
| | 2.5 Verifica delle credenziali | Tutte le credenziali sono verificate con cadenza annuale, in occasione della redazione della DPIA, al fine di controllarne l'effettiva corrispondenza con le mansioni effettivamente svolte. |
| | 2.6 Divieto di lasciare incustodita la postazione di lavoro durante una sessione di trattamento. | L''incaricato viene edotto circa la necessità di non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento. |
| M3 | 3.1 Profilo di autorizzazione per singolo incaricato | Detto processo garantisce, a fronte del superamento della fase di autenticazione, la corretta e completa associazione tra utenza ed oggetti del sistema informatico connessi al profilo assegnato; comprende l'insieme delle informazioni, associate ad una persona, dirette ad individuare a quali dati essa possa accedere ed altresì di quali trattamenti essa possa usufruire; esso stabilisce a quali aree del sistema informatico l'incaricato possa accedere e quali azioni, una voltra entrato, possa compiere. |
| M4 | 4.1 Architettura sicurezza informatica | È previsto un insieme di regole comportamentali e procedure operative dirette a proteggere l'intero sistema informatico.<br>In particolare, esso prevede l'adozione di programmi diretti a prevenire la vulnerabilità degli strumenti elettronici da un lato contrastando gli attacchi esterni dall'altro provvedendo alla correzione dei difetti insiti negli strumenti stessi.<br>In relazione alla correzione dei difetti, esso opera l'aggiornamento costante dei prodotti e la verifica periodica dell'installazione e della configurazione dei prodotti software.<br>In relazione alla tutela da intrusioni esterne in SERVER FARM è posto in essere un IPS (Intrusion Prevention System) a livello perimetrale, gestito dal gruppo Sistemistico di QNT, diretti ad individuare tentativi di introdursi illecitamente nella rete e nei sistemi posti sotto protezione.<br>Gli stessi devono svolgere almeno le seguenti funzioni:<br>* analizzare il traffico di rete secondo i modelli predefiniti dall'amministratore allo scopo di rilevare attività anomale;<br>* segnalare i tentativi di intrusione ed eventualmente<br>* intervenire automaticamente ove possibile con blocco delle connessione<br>Vi è inoltre un sistema di firewall e che filtra le comunicazioni in entrata e in uscita e switch di backend con liste di controllo di accesso. |

| | | |
|---|---|---|
| M5 | 5.1 Procedure di backup | Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza oraria e giornaliera |
| | 5.2 Procedure di ripristino | Sono adottate idonee misure atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni. Sono altresì previste attività indirizzate a ridurre il disservizio in caso di guasto. |
| M6 | 6.1 Policy per l'utilizzo degli strumenti IT | Sono predisposte policy per l'utilizzo degli strumenti elettronici relativamente agli aspetti di:<br>- Utilizzo del Pc;<br>- Navigazione internet<br>- Utilizzo della posta elettronica |
| M7 | 7.1 Piano di Formazione degli incaricati | È previsto un piano di formazione e di aggiornamento per gli incaricati QNT.<br>A tutti i neoassunti viene erogata una formazione di sulla disciplina prevista dal Codice privacy e sulle relative problematiche di applicazione. In occasione dell'inserimento di nuovi strumenti o standard aziendali viene effettuata una formazione a coloro che dovranno applicarli o utilizzarli. |
| M8 | 8.1 Istruzioni agli incaricati | Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. |
| | 8.2 Custodia, uso e riutilizzo supporti rimovibili | Non è permesso l'utilizzo di supporti removibili nel trattamento di dati personali. |
| M9 | 9.1 Procedure automatiche di cancellazione dei dati | Ci sono procedure automatiche di cancellazione dei dati nei seguenti casi:<br>• Log rotation<br>• Backup rotation<br>• Dismissione strumenti elettronici |

## 3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA APPLICATE AL DATA CENTER

- **Certificazioni:** QNT ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza.

L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure chiaramente definiti a presidio dei processi aziendali. Certificazioni: PCI DSS Service Provider Level 1

- Compliance: i processi aziendali di QNT rispondono alle normative vigenti, in particolare per quanto riguarda la rispondenza ai requisiti di privacy. In tale ambito l'azienda ha adeguato il proprio sistema di gestione alle richieste del provvedimento del Garante per la Protezione dei Dati Personali riguardo gli amministratori di sistema. Qualora le prescrizioni di legge vengano modificate QNT adeguerà immediatamente le modalità di erogazione del servizio e le caratteristiche tecniche per essere conforme alle eventuali modifiche.

- Accesso alle informazioni: il sistema di gestione di QNT prevede l'esplicita classificazione del livello di riservatezza di ogni documento. In particolare i documenti contenenti informazioni sui sistemi di sicurezza vengono classificati come riservati e non sono diffusi all'esterno dell'azienda.

- Accesso ai sistemi: gli accessi ai sistemi sono sempre classificabili in accessi di produzione e accessi di amministrazione. Gli accessi di produzione sono quelli oggetto della fornitura del servizio. Gli accessi di amministrazione sono quelli effettuati da QNT o dal cliente con finalità diverse quali la manutenzione, la verifica di anomalie, l'assistenza. Gli accessi di amministrazione da parte di QNT sono riservati a personale con la qualifica ("ruolo") di amministratore di sistema. L'azienda pone particolare attenzione all'assegnazione di tale ruolo soltanto a personale di elevate capacità tecniche e avente caratteristiche di comprovata affidabilità e moralità. L'accesso amministrativo ai sistemi da parte di personale del cliente avverrà attraverso l'assegnazione nominale di personale a ruoli ai quali sono assegnati privilegi di accesso.

- Auditing: nell'ambito del proprio sistema di gestione QNT pone particolare attenzione all'audit dei sistemi e delle attività amministrative compiute sugli stessi. Ogni sistema viene configurato per riportare i propri log di sicurezza verso un sistema centralizzato di elaborazione, classificazione e repository. Tale sistema è in grado di rilevare in tempo reale anomalie sui sistemi. In particolare sono riscontrabili sia eventi singoli che pattern di attività anomale quali serie di login fallite, modifiche massive di password.

- Riservatezza dei dati: il presente documento è stato prodotto assumendo che i dati raccolti dal cliente e presenti sui sistemi ospitati all'interno del Datacenter siano di tipo personale/sensibile, secondo la classificazione prevista dal Codice in materia di protezione dei dati personali.
  In ogni caso QNT non tratterà i dati del Cliente se non per l'unica finalità della loro conservazione ed evenuale trasmissione. QNT non si assume alcuna responsabilità riguardo all'uso che di tali dati viene fatto da parte del cliente o da società incaricate dal cliente stesso che gestiscono o utilizzano il servizio ubicato e gestito nel Datacenter. QNT gestirà e conserverà le informazioni in conformità alle norme espresse dal GDPR.

- Log Management: i log dei sistemi contengono informazioni necessarie alle attività amministrative, di diagnostica e di sicurezza. Ogni sistema viene configurato per loggare ogni evento significativo. I log generati da ogni sistema vengono trasferiti ad un repository centrale che ha il compito di analisi, classificazione e storage. La conservazione dei log avviene secondo le norme di legge, in particolare il Codice Privacy, le norme sulla conservazione dei dati di traffico telematico e quanto previsto dalla certificazione PCI DSS. I log dei sistemi riportano tutte le attività significative ai fini della sicurezza quali gli accessi amministrativi, le modifiche ai permessi e alle configurazioni di sistema e di sicurezza. Il sistema di repository dei log è in grado di generare alert sulla base di eventi o pattern di eventi anomali.

- Crittografia dei dati: La crittografia della base dati avviene sulle credenziali (password) e dati sensibili (le carte di credito).

- Sicurezza dei sistemi: i servizi di sicurezza si ritengono attivi e funzionanti a protezione delle componenti ospitate in Datacenter. I sistemi di protezione sono progettati in modo da massimizzare la protezione e sono amministrati da personale con formazione specifica

- Controlli di sicurezza: sull'intera infrastruttura Datacenter sono svolti Penetration Test e Vulnerability Assessment con cadenza semestrale

- Firewalling: il networking del Datacenter è separato dalle reti pubbliche, dalle altre reti di QNT e dalle altre reti del cliente. I flussi dati tra il networking del Datacenter e l'esterno vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati.

- Intrusion Prevention: il Datacenter è protetto da sistemi di Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso e si comportano in modo trasparente nei confronti del traffico legittimo.

- Filesystem Antivirus: tutti i server che gestiscono dati personali dispongono di moduli Antivirus sul filesystem, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.

- Security Patch Management: la piattaforma è sottoposta ad un processo periodico di verifica delle patch o delle fix rilasciate dai produttori e relativa applicazione ai sistemi.

- Sicurezza fisica: la piattaforma hardware/software Simple Booking fruisce di tutti i servizi di facility management del Datacenter. In particolare Rilevazione fumi e spegnimento incendi. Tutti gli ambienti della FARM sono dotati di rilevatori antifumo e antincendio, con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente.

- Anti intrusione: nel Datacenter è previsto un sistema di anti intrusione integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di TVCC, con il sistema di controllo accessi e con gli allarmi tecnologici.

- Telecamere a circuito chiuso: le telecamere sono posizionate per il controllo del perimetro del datacenter, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.

- Condizionamento: nei Datacenter tutti gli impianti di condizionamento e di raffreddamento sono concepiti per poter smaltire il calore generato dagli apparati. Apposite sonde monitorano in tempo reale temperatura ed umidità e regolano automaticamente gli apparati per garantire sempre le condizioni ottimali di utilizzo.

- Continuità ed emergenza: il Datacenter è stato concepito per fornire affidabilità massima in termini di alimentazione dei server, in quanto ogni rack è connesso a due alimentazioni indipendenti (quadri elettrici attestati su UPS ridondati), in modo tale da permettere la manutenzione delle singole linee di

alimentazione senza creare disservizio e di scongiurare black-out nel caso di fault di una linea di alimentazione.

- Controllo degli accessi fisici al Datacenter: procedure di registrazione degli accessi e identificazione del personale che accede solo se preautorizzato da QNT, accesso alle sale sistemi controllato elettronicamente tramite badge procedure di sicurezza con identificazione ed assegnazione di responsabilità.

## CONNETTIVITÀ DEL DATACENTER

- Linee Internet: l'ampiezza di banda è in grado di fornire il massimo delle performance in ogni circostanza. Ad oggi, al fine di assicurare funzionalità piena anche in caso di malfunzionamenti delle linee Internet di un Provider, il Data Center QNT è collegato in fibra ottica con diversi fornitori di connettività.

- Firewalling: il servizio è gestito tramite sistemi ridondati al 100% prodotti da primari produttori HW internazionali. Gli stessi sono configurati in high availability in modalità Active/Passive. La sicurezza logica è garantita sia a livello perimetrale che tra i sistemi di front-end e il back-end attraverso liste di controllo degli accessi.

- Firewall Perimetrale: i sistemi di firewall perimetrale proteggono il Datacenter QNT dalle minacce provenienti dal mondo Internet. Utilizzando le migliori tecnologie presenti sul mercato sono in grado di garantire, in ogni momento, la massima fruibilità e protezione per i servizi esposti sul web. Il servizio è ridondato in ogni suo componente, assicurando così una continua disponibilità dei sistemi.

- Switch Backend: gli switch di backend forniscono un ulteriore protezione per i dati presenti all'interno del Datacenter QNT. Tali dispositivi garantiscono la sicurezza logica attraverso liste di controllo degli accessi. Il servizio, ridondato in ogni suo componente, è in grado di fornire le massime performance abbinate alla massima disponibilità.

- Sistema anti-intrusione: identifica l'insieme delle strumentazioni hardware e delle configurazioni software che permettono di "tracciare" l'accesso a particolari servizi e fornire, su richiesta, l'elenco degli accessi effettuati su un particolare sistema e/o un particolare servizio.

- IPS: il sistema IPS (Intrusion Prevention System) è in grado di bloccare automaticamente gli attacchi rilevati, fornendo così una protezione real-time ai servizi erogati dal Datacenter QNT.

- Linee di comunicazione: le soluzioni ed i servizi proposti sono erogati tramite connessione Internet protetta (https). Tutti i dati personali degli utenti vengono trasmessi esclusivamente su connessioni protette.

QNT S.r.l. Socio Unico