Carta bianca sulla sicurezza dei dati di MyQ Roger 2.x

ITALIANO

Generato da docs.myq-solution.com
agosto/2026
Copyright © 2026 MyQ spol. s r.o. Tutti i diritti riservati.

Avviso sulla traduzione

Questa traduzione è stata realizzata con l’assistenza dell’intelligenza artificiale. In caso di discrepanze o ambiguità, fa fede il documento originale in lingua inglese.

Indice

1 Introduzione 5
2 Glossario 6
3 Sicurezza delle operazioni 7
3.1 Introduzione 7
3.2 Monitoraggio 7
3.3 Gestione delle vulnerabilità 9
3.4 Sicurezza dell'infrastruttura 9
3.5 Flusso di lavoro di sviluppo 10
3.6 Conclusione 11
4 Sicurezza delle applicazioni 12
4.1 L'evoluzione delle minacce alla sicurezza 12
4.2 L'approccio alla sicurezza di MyQ Roger 12
4.3 Shifting Left nella sicurezza 13
4.4 Responsabilità di sicurezza di MyQ 13
4.5 Controllo/gestione della sicurezza MyQ Roger 13
4.6 Microsoft Azure e conformità 14
4.7 Responsabilità dei clienti in materia di sicurezza 14
4.8 Automazione della sicurezza 15
4.9 Conclusione 15
5 Protezione dei dati 17
5.1 Panoramica 17
5.2 Sicurezza cloud multi-tenant 17
5.3 Crittografia e comunicazione sicura 17
5.4 Conformità e gestione delle identità 17
5.5 Conformità al GDPR 18
5.6 Backup dei dati 18
6 Informativa sulla privacy 20
6.1 1. Dati che raccogliamo o riceviamo 20
6.2 2. Come utilizziamo i dati 22
6.3 3. Base giuridica 23
6.4 4. Periodi di conservazione 24
6.5 5. Condivisione dei dati personali per scopi legali e commerciali 24
6.6 6. Statistiche anonime 26

6.7 7. Comunicazioni di marketing 26
6.8 8. Sicurezza e ubicazione dei dati dell'utente 27
6.9 9. I vostri diritti 27
6.10 10. Contattaci 30
7 Uptime del server, backup dei dati e disaster recovery 31
7.1 Tempo di attività del server 31
7.2 Monitoraggio dello stato del sistema in tempo reale 31
7.3 Strategie di backup 31
7.4 Scenari di emergenza e piano di risposta 32
8 Fiducia zero 33
8.1 Comprendere la sicurezza Zero Trust 33
8.2 Che cos'è Zero Trust? 33
8.3 Come Zero Trust si applica a MyQ Roger 34
8.4 Affrontare le minacce informatiche con Zero Trust 35
8.5 Considerazioni relative alla conformità e alle normative 35
8.6 Perché Zero Trust è importante 35
9 Accesso sicuro con MyQ Roger 36
9.1 Introduzione 36
9.2 Autenticazione sicura con MyQ Roger 36
9.3 Autenticazione con PIN legacy 36
9.4 Responsabilità in materia di sicurezza 37
9.5 Conclusione 37
10 Stampa sicura con MyQ Roger 38
10.1 La sfida della stampa sicura 38
10.2 MyQ Roger: una soluzione completa per la stampa sicura 38
10.3 Metodi di stampa sicuri in MyQ Roger 38
10.4 Conclusione 39
11 Contatti commerciali 40

1 Introduzione

Lo scopo di questo documento è informare i clienti di MyQ Roger sui processi che comportano la creazione di connessioni nel sistema e sulle misure di sicurezza adottate per proteggere il conseguente trasferimento dei dati.

Sono trattati i seguenti argomenti:

- Glossario: una sintesi della terminologia utilizzata.
- Sicurezza delle operazioni: esamina attentamente i sistemi di monitoraggio, l'infrastruttura e i flussi di lavoro di sviluppo per garantire la sicurezza di MyQ Roger.
- Sicurezza delle applicazioni: delinea l'approccio alla sicurezza di MyQ Roger, descrivendo in dettaglio le responsabilità delle varie parti, l'automazione e la gestione.
- Protezione dei dati: riassume gli standard di MyQ Roger per la sicurezza cloud multi-tenant, la crittografia e la comunicazione sicura, la conformità e la gestione delle identità. Contiene anche disposizioni relative alla conformità al GDPR e al backup dei dati.
- Tempo di attività del server, backup dei dati e ripristino di emergenza: descrive in dettaglio il monitoraggio dello stato fornito da MyQ Roger e le strategie di backup e i piani di risposta disponibili.
- Zero Trust: esamina il significato e l'importanza della sicurezza zero trust e delinea come MyQ Roger rispetta questi principi.
- Accesso sicuro con MyQ Roger: descrive in dettaglio le misure adottate da MyQ Roger per garantire la sicurezza dell'accesso.
- Stampa sicura con MyQ Roger: fornisce dettagli sui vari metodi di stampa utilizzati da MyQ Roger e sulle misure di sicurezza che accompagnano ciascuno di essi.

2 Glossario

- **IPP/s (Internet Printing Protocol over Secure TLS)**:
  - MyQ Roger garantisce una stampa sicura utilizzando il protocollo di stampa Internet (IPP) su un canale crittografato TLS, impedendo l'accesso non autorizzato e garantendo l'integrità dei dati in transito.
  - MyQ Roger ottimizza il traffico di rete attraverso una gestione efficiente dei pacchetti, riducendo la trasmissione di dati non necessari e garantendo una comunicazione sicura tra gli endpoint.
- **TLS (Transport Layer Security)**:
  MyQ Roger applica TLS 1.2/1.3 per la crittografia sicura dei dati in tutte le comunicazioni, garantendo la protezione contro le intercettazioni e gli attacchi man-in-the-middle (MITM).
- **Dati inattivi, dati in transito**:
  - **Dati inattivi**: MyQ Roger crittografa i dati memorizzati utilizzando AES-256, garantendo che le informazioni sensibili rimangano protette da accessi non autorizzati.
  - **Dati in transito**: tutti i dati trasferiti tra client, server e servizi cloud sono crittografati utilizzando TLS per mantenere l'integrità e la riservatezza.
- **Infrastruttura Zero Trust**:
  MyQ Roger segue un modello di sicurezza **Zero Trust** implementando l'autenticazione continua, la verifica dei dispositivi e l'accesso con privilegi minimi per utenti e servizi.
- **IAM (Identity and Access Management)**:
  MyQ Roger integra le migliori pratiche IAM applicando l'autenticazione sicura degli utenti, l'autenticazione a più fattori (MFA) e i controlli di accesso basati sull'identità.
- **RBAC (controllo degli accessi basato sui ruoli)**:
  MyQ Roger implementa l'RBAC per limitare le autorizzazioni in base ai ruoli degli utenti, garantendo che solo il personale autorizzato possa accedere alle funzioni critiche e ai dati sensibili.
- **SSO (Single Sign-On)**:
  MyQ Roger supporta **l'SSO** tramite l'integrazione OAuth2, consentendo un'autenticazione senza soluzione di continuità tra le applicazioni aziendali, mantenendo al contempo la sicurezza e la conformità.

3 Sicurezza delle operazioni

3.1 Introduzione

La sicurezza è una priorità assoluta per MyQ Roger. Adottiamo un approccio **che mette al primo posto la sicurezza** in ogni fase dello sviluppo, dell'implementazione e delle operazioni. Data la natura critica degli ambienti cloud, la sicurezza deve essere **proattiva, automatizzata e monitorata continuamente** per prevenire violazioni e accessi non autorizzati.

La nostra **strategia di operazioni sicure** integra **monitoraggio continuo, gestione delle vulnerabilità, sicurezza dell'infrastruttura e conformità** per garantire l'integrità delle applicazioni e dell'infrastruttura.

3.2 Monitoraggio

Il monitoraggio continuo è essenziale per rilevare e rispondere alle minacce in tempo reale. MyQ implementa un **approccio di monitoraggio multilivello:**

3.2.1 Rilevamento e risposta degli endpoint (EDR)

- Monitora tutti gli endpoint (server, VM e container) alla ricerca di attività sospette.
- Utilizza **l'analisi comportamentale e le informazioni sulle minacce** per rilevare le minacce avanzate.
- Isola automaticamente gli endpoint compromessi per impedire il movimento laterale.

3.2.2 Azure Defender (ora Defender for Cloud)

- Protegge **Azure AKS, SQL Server, macchine virtuali e archiviazione**.
- Fornisce **rilevamento delle minacce in tempo reale** e consigli sulla configurazione della sicurezza.
- Si integra con **Microsoft Sentinel (SIEM)** per avvisi centralizzati.

3.2.3 Scansione host

- Esegue la scansione di **macchine virtuali, istanze cloud e server locali** alla ricerca di configurazioni errate e software obsoleti.
- Rileva **i rischi di escalation dei privilegi, i punti di accesso non autorizzati e le dipendenze obsolete**.

3.2.4 Raccolta e analisi dei log

- **Registrazione centralizzata** su un cluster separato per garantire scalabilità e isolamento.
- **I log provenienti da Kubernetes, dalle applicazioni e dall'infrastruttura** vengono etichettati per un recupero efficiente.
- **Le politiche di conservazione a lungo termine** garantiscono la conformità e l'analisi della sicurezza.
- **I meccanismi di allerta** rilevano anomalie e incidenti di sicurezza, integrandosi con SIEM.
- **Correlazione dei log in tempo reale** per richieste API, eventi di autenticazione, query di database e traffico firewall.

3.2.5 Scansione delle porte

- Rileva **le porte aperte** non autorizzate che espongono i servizi a minacce.
- Utilizza **strumenti automatizzati come Nmap e ZMap** per eseguire la scansione alla ricerca di **modifiche inattese delle porte**.

3.2.6 Scansione dei container

- **Scansione statica e dinamica** dei container Docker prima della distribuzione.
- Identifica le vulnerabilità nelle **immagini di base, nei livelli applicativi e nelle autorizzazioni di runtime**.
- Integrato con **Trivy** per **la scansione di sicurezza delle immagini**.

3.2.7 Monitoraggio Kubernetes

- Utilizza **il monitoraggio integrato di Azure Kubernetes Service (AKS)** con **Prometheus e Grafana**.
- Monitora **le chiamate API Kubernetes, le politiche RBAC e la sicurezza dei pod**.
- Avvisa in caso di **escalation dei privilegi dei container, utilizzo eccessivo delle risorse e tentativi di movimento laterale.**

3.2.8 Scansioni TLS regolari

- MyQ esegue **scansioni di sicurezza TLS utilizzando Qualys SSL Labs** per garantire le migliori pratiche.
- Le configurazioni TLS vengono valutate per mantenere un **rating di sicurezza A+**, mitigando i rischi derivanti da protocolli deboli.
- Strumenti automatizzati verificano **la validità dei certificati, il monitoraggio della scadenza e la forza del protocollo**.

3.3 Gestione delle vulnerabilità

3.3.1 Scansione delle vulnerabilità

- **Scansioni regolari** rilevano falle di sicurezza nelle applicazioni e nell'infrastruttura.
- Include **la scansione CVE automatizzata** per i componenti distribuiti nel cloud.
- Si integra con **DefectDojo, SonarQube e Trivy** per la valutazione dei rischi.

3.3.2 Test di penetrazione

- Condotti regolarmente per identificare le vulnerabilità di sicurezza prima che vengano sfruttate.
- Combina **metodologie di test automatizzate e manuali** per una valutazione completa.
- I risultati vengono **documentati, classificati in ordine di priorità e corretti** di conseguenza.

3.4 Sicurezza dell'infrastruttura

Un'**infrastruttura rinforzata** garantisce una sicurezza che va oltre il semplice monitoraggio. MyQ utilizza:

3.4.1 SIEM (Security Information and Event Management)

- **Microsoft Sentinel SIEM** raccoglie gli eventi di sicurezza per il rilevamento in tempo reale.
- Analizza i registri dei **firewall, dei sistemi di identità, delle applicazioni, degli audit e delle minacce**.
- Consente **risposte automatizzate alle minacce rilevate**.

3.4.2 Monitoraggio e gestione della sicurezza

- **Il database dei bug Jira** traccia, classifica e assegna priorità alle vulnerabilità di sicurezza.
- **DefectDojo** consolida i risultati dei test, garantendo un monitoraggio strutturato degli impegni di sicurezza.
- **L'applicazione** regolare **di patch e la correzione dei difetti** mantengono un elevato livello di sicurezza.

3.4.3 Gestione delle identità e degli accessi (IAM)

- Applica **il modello Zero Trust** con **il controllo degli accessi basato sui ruoli (RBAC) e l'autenticazione a più fattori (MFA)**.
- Utilizza **Azure AD** per la governance delle identità.

- **Gli avvisi di escalation dei privilegi** rilevano gli accessi amministrativi non autorizzati.

3.5 Flusso di lavoro di sviluppo

Lo sviluppo sicuro del software è un aspetto fondamentale della strategia di sicurezza di MyQ. Le seguenti misure garantiscono l'integrità del codice, delle pipeline e degli ambienti cloud:

3.5.1 Ambiente di sviluppo sicuro

- Gli sviluppatori MyQ utilizzano **ambienti** con **protezione avanzata** e protezione degli endpoint.
- Gli sviluppatori devono seguire **pratiche di codifica sicure e seguire regolarmente corsi di formazione sulla sicurezza**.

3.5.2 Pipeline sicure GitLab

- Le pipeline CI/CD di GitLab includono **controlli di sicurezza automatizzati, revisioni del codice e test**.
- **I test di sicurezza statici delle applicazioni (SAST)** e **i test di sicurezza dinamici delle applicazioni (DAST)** rilevano le vulnerabilità.
- **La firma delle immagini dei container** garantisce che vengano distribuite solo immagini affidabili.

3.5.3 IAM e controllo degli accessi

- Solo **il personale DevOps e SecOps selezionato** ha accesso agli ambienti cloud Azure.
- Viene applicato **il controllo degli accessi basato sui ruoli (RBAC) con elevazione dei privilegi minimi Just-In-Time (JIT)**.

3.5.4 Azure Kubernetes e sicurezza dei container

- **I cluster AKS** di MyQ **estraggono le immagini solo da Azure Container Registry (ACR)**.
- Gli ambienti AKS applicano **criteri di rete e Pod Security Standards (PSS)** per isolare i carichi di lavoro.

3.5.5 Gestione dei segreti

- **Tutti i segreti e le chiavi API sono archiviati in Azure Key Vault**, accessibile solo al personale autorizzato IAM.
- Prima del commit su Git vengono eseguite **scansioni del filesystem Trivy** per rilevare e prevenire segreti sensibili.

3.6 Conclusione

La strategia di operazioni sicure di MyQ si basa su un **monitoraggio continuo, una gestione proattiva delle minacce e una solida sicurezza dell'infrastruttura**. Sfruttando **strumenti di sicurezza avanzati, controlli di accesso rigorosi e test automatizzati**, MyQ garantisce un **ambiente cloud sicuro e resiliente**.

Con l'**integrazione di scansioni di sicurezza TLS, test di penetrazione e registrazione centralizzata**, MyQ migliora la sua capacità di **rilevare, rispondere e mitigare** efficacemente **i rischi per la sicurezza**.

La sicurezza è una **sfida in continua evoluzione** e MyQ rimane impegnata a **migliorare le misure di sicurezza attraverso aggiornamenti regolari, audit di conformità e best practice di sicurezza**. Mantenendo un **approccio incentrato sulla sicurezza**, MyQ garantisce l'**integrità e la riservatezza** dei propri servizi, assicurando **fiducia e affidabilità** a tutte le parti interessate.

4 Sicurezza delle applicazioni

4.1 L'evoluzione delle minacce alla sicurezza

All'inizio, prima che Internet fosse diffuso, le stampanti erano collegate direttamente tramite cavi LPT e le preoccupazioni relative alla sicurezza erano minime. Il rischio maggiore era di natura fisica: qualcuno che guardava da dietro le spalle dell'utente per vedere i documenti stampati. Il panorama della sicurezza era semplice e le minacce informatiche erano praticamente inesistenti.

Tuttavia, con la connessione in rete di stampanti e dispositivi, il panorama delle minacce è cambiato drasticamente. Ora che le stampanti sono accessibili tramite reti locali (LAN) e persino Internet, gli aggressori non hanno più bisogno di un accesso fisico. Minacce come gli attacchi man-in-the-middle (MITM), l'intercettazione non autorizzata di dati e gli exploit remoti sono diventati prevalenti. I criminali informatici si sono evoluti dal guardare alle spalle al intercettare il traffico di rete e sfruttare le vulnerabilità.

Mitigare questi rischi è una sfida continua, poiché nuove minacce emergono frequentemente. Per affrontare queste sfide di sicurezza in continua evoluzione, MyQ Roger implementa pratiche di sicurezza continue, monitoraggio proattivo e robusti meccanismi di difesa.

4.2 L'approccio alla sicurezza di MyQ Roger

MyQ Roger è stato progettato con un approccio che mette al primo posto la sicurezza, garantendo che l'innovazione e l'esperienza dell'utente siano sempre in linea con i più elevati standard di sicurezza. Il nostro impegno per la sicurezza si riflette nei nostri continui sforzi per integrare misure di sicurezza robuste in ogni fase dello sviluppo. Adottiamo una filosofia "sicura di default", incorporando la sicurezza nei nostri prodotti e servizi fin dall'inizio.

Per raggiungere questo obiettivo, MyQ Roger sfrutta l'automazione, le valutazioni dei rischi basate sui dati e le migliori pratiche di sicurezza per identificare e mitigare in modo proattivo le minacce. Implementando i controlli di sicurezza nelle prime fasi del ciclo di sviluppo, seguendo un **approccio shift-left**, garantiamo che le vulnerabilità vengano rilevate e risolte prima che raggiungano la produzione. Questa integrazione proattiva ci consente di scalare in modo efficiente, ridurre i rischi e minimizzare le minacce alla sicurezza. Il nostro approccio rafforza la nostra dedizione alla protezione dei dati dei clienti, dei flussi di lavoro e della sicurezza complessiva.

4.3 Shifting Left nella sicurezza

Lo spostamento a sinistra della sicurezza significa integrare la sicurezza nelle prime fasi del ciclo di vita dello sviluppo del software (SDLC) piuttosto che affrontare le vulnerabilità in un secondo momento. Individuando i problemi di sicurezza nelle fasi iniziali di sviluppo, preveniamo costose correzioni e mitighiamo potenziali violazioni. Questa strategia proattiva garantisce che ogni riga di codice soddisfi i più elevati standard di sicurezza prima di raggiungere la produzione, riducendo i rischi e rafforzando la nostra posizione di sicurezza complessiva.

4.4 Responsabilità di sicurezza di MyQ

MyQ Roger si impegna a proteggere i dati dei clienti e a garantire un ambiente operativo sicuro. Le nostre principali responsabilità in materia di sicurezza includono:

- **Protezione dei dati**: MyQ garantisce che i dati dei clienti siano archiviati e crittografati in modo sicuro, impedendo accessi non autorizzati e garantendo la riservatezza dei dati.
- **Applicazione regolare di patch di sicurezza**: applichiamo in modo proattivo patch di sicurezza e aggiornamenti a tutti i sistemi per eliminare le vulnerabilità prima che possano essere sfruttate.
- **Gestione del controllo degli accessi**: applichiamo politiche di accesso rigorose seguendo il principio del privilegio minimo, garantendo che solo il personale autorizzato possa accedere alle risorse sensibili.

Sostenendo questi principi di sicurezza, MyQ Roger promuove una cultura della sicurezza, proteggendo gli utenti da potenziali minacce e garantendo al contempo la conformità agli standard del settore.

4.5 Controllo/gestione della sicurezza MyQ Roger

Pur affidandoci a un'infrastruttura cloud sicura, MyQ Roger si assume la responsabilità diretta di implementare ulteriori livelli di sicurezza e di aderire alle migliori pratiche del settore. Il nostro approccio include:

- **Gestione delle chiavi con Azure Key Vault**: utilizziamo Azure Key Vault per archiviare e gestire in modo sicuro tutti i segreti, le chiavi private e i certificati, garantendo controlli di accesso rigorosi e crittografia.
- **Certificazione ISO 27001**: aderiamo agli standard ISO 27001 per mantenere un approccio strutturato e coerente alla sicurezza delle informazioni.
- **Rilevamento e risposta degli endpoint (EDR)**: sfruttiamo soluzioni EDR avanzate per rilevare, analizzare e mitigare le minacce alla sicurezza in tempo reale, riducendo i tempi di risposta e minimizzando i rischi.

- **Pratiche di sviluppo sicuro**: il nostro ciclo di vita di sviluppo software sicuro include valutazioni delle vulnerabilità, monitoraggio continuo e scansioni di sicurezza automatizzate per rilevare e correggere i difetti di sicurezza.
- **Audit di sicurezza regolari**: conduciamo audit interni e di terze parti per garantire la conformità e affrontare in modo proattivo i rischi per la sicurezza.
- **SIEM con Azure Sentinel**: utilizziamo Azure Sentinel per il rilevamento delle minacce in tempo reale, la risposta automatizzata e il monitoraggio continuo della sicurezza in tutti gli ambienti cloud e di rete.

Implementando queste misure di sicurezza, MyQ Roger rafforza il proprio quadro di sicurezza complessivo, garantendo che i dati dei clienti rimangano protetti in ogni momento.

4.6 Microsoft Azure e conformità

MyQ Roger funziona su Microsoft Azure, sfruttando Azure Kubernetes Service (AKS), Azure SQL Server e Azure Cosmos DB per MongoDB. Operando all'interno dell'infrastruttura di Azure, beneficiamo degli standard di sicurezza, conformità e affidabilità leader del settore di Microsoft.

4.6.1 Responsabilità di Microsoft in materia di sicurezza e conformità

- Azure aderisce a framework di conformità globali come ISO 27001, SOC 2 e GDPR nell'UE, garantendo il rispetto di rigorosi standard normativi.
- Microsoft fornisce funzionalità di sicurezza integrate come l'isolamento della rete, la protezione dell'identità e il rilevamento continuo delle minacce, riducendo le superfici di attacco.
- I servizi Azure sono sottoposti a rigorose valutazioni di sicurezza e test di penetrazione per identificare e correggere in modo proattivo le vulnerabilità.

Sfruttando l'infrastruttura sicura di Azure, MyQ Roger aggiunge i propri livelli di sicurezza per creare un modello di sicurezza robusto e resiliente che protegge le applicazioni e i dati dei clienti.

4.7 Responsabilità dei clienti in materia di sicurezza

Sebbene MyQ Roger fornisca un'infrastruttura sicura e misure di sicurezza di prim'ordine, anche i clienti hanno responsabilità fondamentali per garantire la sicurezza del proprio ambiente. Queste includono:

- **Mantenimento di un elenco di utenti attivi**: i clienti devono gestire continuamente l'accesso degli utenti sfruttando la sincronizzazione automatica degli utenti o disabilitando manualmente gli account inattivi per ridurre al minimo i rischi.

- **Applicazione del controllo degli accessi basato sui ruoli (RBAC)**: i clienti devono applicare i principi RBAC per limitare l'accesso degli utenti solo alle autorizzazioni necessarie, garantendo una maggiore sicurezza ed efficienza operativa.
- **Protezione della rete locale**: anche se MyQ Roger opera con un modello zero-trust, i clienti devono garantire che la loro rete locale rispetti le migliori pratiche di sicurezza, come le configurazioni firewall, la segmentazione della rete e la protezione degli endpoint.
- **Corretta manutenzione delle risorse**: tutti i dispositivi collegati, comprese le stampanti e i dispositivi multifunzione (MFP), devono essere aggiornati regolarmente con il firmware e le patch di sicurezza più recenti per prevenire vulnerabilità.

Aderendo a queste responsabilità, i clienti rafforzano la loro posizione di sicurezza beneficiando al contempo del quadro di sicurezza completo di MyQ Roger.

4.8 Automazione della sicurezza

Per migliorare ulteriormente la sicurezza durante tutto il ciclo di vita dello sviluppo, MyQ Roger integra test di sicurezza automatizzati e valutazioni di sicurezza esterne:

- **SAST (Static Application Security Testing)**: condotto su ogni commit per rilevare le vulnerabilità di sicurezza nelle prime fasi del ciclo di sviluppo, riducendo la probabilità che codice non sicuro raggiunga la produzione.
- **DAST (Dynamic Application Security Testing)**: eseguito in ambienti sandbox per identificare e mitigare i rischi di sicurezza in fase di esecuzione prima della distribuzione.
- **Test di penetrazione esterni**: ci avvaliamo di esperti di sicurezza indipendenti per eseguire test di penetrazione, garantendo che le nostre difese di sicurezza siano in grado di resistere a scenari di attacco reali.

Automatizzando i test di sicurezza e conducendo regolari valutazioni esterne, MyQ Roger mantiene un approccio proattivo e resiliente alla sicurezza.

4.9 Conclusione

In MyQ Roger, la sicurezza non è un ripensamento, ma parte integrante del nostro prodotto e del ciclo di vita dello sviluppo. Combinando principi di sicurezza intrinseca, best practice del settore e un solido framework di conformità, forniamo una posizione di sicurezza robusta che protegge i dati e le operazioni dei nostri clienti. Il nostro impegno per il miglioramento continuo della sicurezza garantisce che MyQ Roger rimanga resiliente alle minacce in continua evoluzione, mantenendo i più elevati standard di affidabilità e fiducia. Continueremo a evolvere la nostra strategia

di sicurezza, adattandoci alle nuove sfide e sfruttando le ultime tecnologie per sostenere la nostra missione di fornire un'esperienza utente sicura e senza interruzioni.

5 Protezione dei dati

5.1 Panoramica

La protezione dei dati è al centro dell'approccio alla sicurezza **di MyQ Roger**, che garantisce che ogni aspetto della sua soluzione di stampa e scansione basata su cloud sia conforme ai più elevati standard del settore. Un principio fondamentale di MyQ Roger è che **nessun dato relativo ai lavori di stampa o scansione venga mai trasferito attraverso i suoi server**. MyQ Roger limita invece rigorosamente la raccolta dei dati ai **metadati** essenziali, come **i nomi dei file di lavoro, le dimensioni dei file e le informazioni sul numero di pagine**. Ciò garantisce l'efficienza operativa salvaguardando al contempo la privacy degli utenti.

5.2 Sicurezza cloud multi-tenant

Essendo un **prodotto cloud multi-tenant**, MyQ Roger offre ai clienti un ambiente **logicamente isolato** per impedire l'esposizione dei dati tra tenant.

Per garantire la resilienza, MyQ Roger si affida ad **Azure SQL** e **Azure Cosmos DB**, che offrono entrambi funzionalità di sicurezza integrate come **la crittografia dei dati inattivi e in transito, il rilevamento automatico delle minacce e il monitoraggio degli accessi**. L'infrastruttura cloud è sottoposta a continue valutazioni di sicurezza per mitigare i rischi associati agli ambienti multi-tenant.

5.3 Crittografia e comunicazione sicura

La sicurezza è integrata in ogni livello delle operazioni di MyQ Roger. Tutte le comunicazioni tra client, servizi cloud e stampanti sono **crittografate utilizzando TLS (Transport Layer Security)** per impedire accessi non autorizzati o manomissioni.

Per rafforzare ulteriormente la sicurezza, tutte le certificazioni utilizzate all'interno di MyQ Roger sono firmate da **autorità di certificazione (CA) pubblicamente affidabili**, garantendo il massimo livello di affidabilità. Inoltre, le certificazioni vengono **sostituite ogni tre mesi**, riducendo il rischio di potenziali compromissioni e mantenendo la conformità alle migliori pratiche di sicurezza.

5.4 Conformità e gestione delle identità

MyQ Roger è conforme agli standard di sicurezza riconosciuti a livello internazionale e possiede **la certificazione ISO 27001**, a dimostrazione del suo impegno nell'implementazione di solide pratiche di gestione della sicurezza delle informazioni.

Per applicare controlli di accesso rigorosi, viene implementato **il controllo degli accessi basato sui ruoli (RBAC)**, che garantisce che agli utenti vengano concesse **solo le autorizzazioni necessarie per il loro ruolo**. Ciò riduce al minimo l'esposizione a dati sensibili e riduce il rischio di uso improprio accidentale o intenzionale.

5.5 Conformità al GDPR

Garantire la conformità al **Regolamento generale sulla protezione dei dati (GDPR)** è una priorità assoluta per MyQ Roger. In conformità con i principi del GDPR, MyQ Roger segue rigorose misure di protezione dei dati per salvaguardare la privacy degli utenti:

- **Minimizzazione dei dati**: vengono raccolti solo i metadati essenziali, eliminando il rischio di archiviare documenti sensibili degli utenti.
- **Diritti e controllo degli utenti**: gli utenti hanno la possibilità di richiedere **l'accesso, la correzione, la cancellazione o l'anonimizzazione** dei propri dati personali, come previsto dal GDPR.
- **Trasparenza nel trattamento dei dati**: politiche sulla privacy chiare e concise descrivono come vengono gestiti, archiviati e protetti i metadati.
- **Archiviazione sicura dei dati**: tutti i dati sono **crittografati sia in fase di archiviazione che di trasmissione**, garantendo la piena conformità ai rigorosi requisiti di sicurezza del GDPR.
- **Misure di anonimizzazione**: quando necessario, MyQ Roger implementa **tecniche di anonimizzazione dei dati** per garantire che i dati personali non possano più essere attribuiti a un utente specifico, rafforzando la protezione della privacy.

Queste misure garantiscono che MyQ Roger sia pienamente conforme ai requisiti fondamentali del GDPR, offrendo agli utenti il controllo sui propri dati personali e mantenendo al contempo un ambiente sicuro e conforme.

5.6 Backup dei dati

Per proteggere dalla perdita di dati e garantire l'affidabilità del servizio, MyQ Roger implementa una **strategia completa di backup dei dati**. Ciò include:

- **Backup automatici**: **backup incrementali e completi** programmati regolarmente garantiscono che i dati rimangano recuperabili in caso di incidente.
- **Archiviazione sicura**: i backup sono crittografati utilizzando **la crittografia AES-256**, garantendo che anche nel caso improbabile di un accesso non autorizzato, i dati rimangano illeggibili.

- **Politiche di conservazione**: i backup vengono **conservati per un periodo definito** in linea con i requisiti di conformità, consentendo un recupero efficiente in caso di guasti del sistema o scenari di ripristino di emergenza.
- **Test e verifica dell'integrità**: vengono condotti regolarmente **test di integrità dei backup** per confermare che i backup archiviati siano funzionali e affidabili, garantendo un ripristino dei dati senza interruzioni quando necessario.

Implementando queste solide misure di sicurezza, conformità e backup, **MyQ Roger fornisce una soluzione di stampa e scansione basata su cloud sicura, privata e altamente efficiente** che soddisfa i più elevati standard di protezione dei dati del settore.

6 Informativa sulla privacy

La tua privacy è importante per noi e la prendiamo molto sul serio. La presente Informativa sulla privacy per MyQ Roger Solution (l'"Informativa sulla privacy") spiega quali tipi di informazioni MyQ può raccogliere, conservare ed elaborare in relazione alla fornitura di prodotti, servizi, contenuti, applicazioni o altri componenti che fanno parte di MyQ Roger Solution (i "Servizi") e come tali informazioni vengono utilizzate e protette. Descrive inoltre come contattarci in caso di domande o dubbi relativi ai dati personali.

La presente Informativa sulla privacy è pubblicata da MyQ, spol. s.r.o., con sede legale in Českomoravská 2420/15, Libeň, 190 00 Praha 9, Repubblica Ceca, numero di identificazione aziendale 615 06 133, iscritta al Registro delle Imprese tenuto dal Tribunale Municipale di Praga, sezione C, inserto 29842 ("MyQ" o "noi").

Ci riserviamo il diritto di apportare modifiche alla presente Informativa sulla privacy in qualsiasi momento. Si prega di controllare periodicamente l'Informativa sulla privacy per eventuali modifiche, anche se, se sei nostro cliente, potremmo anche comunicarti via e-mail eventuali modifiche che, a nostra esclusiva discrezione, hanno un impatto significativo sul tuo utilizzo dei Servizi o sul modo in cui trattiamo i tuoi dati personali. L'uso continuato dei nostri Servizi coperti dalla presente Informativa sulla privacy implica l'accettazione di tutte le modifiche apportate di volta in volta alla presente Informativa sulla privacy.

6.1 1. Dati che raccogliamo o riceviamo

Raccogliamo dati personali dai nostri clienti, in qualità di utenti dei Servizi, e dai loro utenti finali (che includono i dipendenti dei nostri clienti) al fine di configurare e gestire gli account degli utenti e fornire e amministrare i Servizi. Raccogliamo anche dati e metriche di utilizzo. Siamo i titolari del trattamento di questi dati personali.

Per quanto riguarda i dati personali che possono essere inclusi nei metadati dei Contenuti, come definiti nei Termini di servizio https://www.myq-solution.com/en/myq-legal-documents , che gli utenti o gli utenti finali gestiscono utilizzando i Servizi, o per quanto riguarda i dati personali a cui potremmo avere accesso durante la fornitura di servizi di assistenza remota o locale (i "Dati dei clienti"), trattiamo tali dati personali per conto dei nostri clienti in qualità di responsabili del trattamento dei dati. Quando trattiamo i Dati dei clienti per fornire i Servizi ai nostri clienti, agiamo in conformità con le istruzioni dei nostri clienti in qualità di loro responsabili del trattamento dei dati. Conserviamo sempre i Dati dei clienti che trattiamo per

conto dei nostri clienti e in conformità con le loro istruzioni separatamente dai dati degli altri nostri clienti e li manteniamo strettamente riservati.

6.1.1 1.1 Dati degli utenti e degli utenti finali dei nostri Servizi

Raccogliamo i tuoi dati personali quando:

- Creiamo un account all'interno dei nostri Servizi;
- Accedete al nostro Servizio, inserendo il vostro nome utente (e-mail) e la vostra password;
- Utilizzi i nostri Servizi o interagisci in altro modo con MyQ, ad esempio quando ci invii delle richieste;
- Fornite volontariamente tali dati a MyQ in altro modo.

Quando crei un account con MyQ, ti chiederemo di compilare un modulo di registrazione indicando il tuo nome, cognome, e-mail, azienda e titolo di lavoro. Puoi anche scegliere di aggiungere un numero di telefono al tuo account.

Raccogliamo e trattiamo anche il tuo nome utente (e-mail) e la tua password.

Ai fini dell'analisi e del miglioramento dei nostri Servizi, i nostri server possono registrare automaticamente le informazioni quando l'utente visita il nostro sito web o utilizza alcuni dei nostri Servizi ("dati di utilizzo"), tra cui:

- Informazioni sui servizi di terze parti che l'utente e i suoi utenti finali collegano ai Servizi per scopi di autenticazione e connessione all'archiviazione cloud dell'utente;
- Informazioni sui dispositivi dell'utente, ad esempio il tipo e la marca delle stampanti e il loro numero di serie;
- Informazioni sull'utilizzo dei nostri Servizi, ad esempio la quantità di documenti stampati o scansionati.

I Servizi consentono all'utente di connettersi ad applicazioni di terze parti o altri servizi, ad esempio One Drive o Google Disk, allo scopo di condividere documenti e altri Contenuti con i Servizi. Se l'utente sceglie di connettersi a servizi di terze parti, chiederemo il suo permesso per consentire ai Servizi di accedere a tali servizi di terze parti, tuttavia MyQ non tratterà alcun dato personale ivi memorizzato, ad eccezione dei Dati del Cliente, come definiti sopra.

Se i nostri Servizi vengono acquistati da un'entità, sono i singoli utenti all'interno dell'organizzazione di tale entità che accedono alla nostra piattaforma di Servizi e i cui dati personali vengono raccolti, come descritto sopra. Laddove tale entità ci fornisca direttamente i dati personali dei propri dipendenti o di altri singoli utenti che ha autorizzato ad accedere ai Servizi, essa deve disporre di tutti i consensi, le

autorizzazioni o le registrazioni necessari per trattare e fornirci i dati personali dei propri dipendenti o utenti.

6.1.2 1.2 Dati dei clienti

Per fornire i nostri Servizi ai nostri utenti e utenti finali, potremmo anche trattare i Dati dei clienti, come definiti sopra. Il trattamento dei Dati dei clienti è soggetto alla politica sulla privacy degli utenti, i quali sono tenuti a garantire che il trattamento di tali dati sia lecito e conforme alla legge applicabile. Il trattamento dei dati relativi ai Dati dei clienti effettuato da MyQ è regolato dagli accordi sul trattamento dei dati applicabili stipulati con gli utenti.

6.2 2. Come utilizziamo i dati

Utilizziamo i vostri dati personali per i seguenti scopi:

6.2.1 2.1 Per fornire i Servizi

Potremmo trattare i vostri dati personali per identificarvi quando accedete al vostro account e utilizzate i nostri Servizi, per consentirci di gestire i Servizi e fornirveli. Ciò può includere la verifica dei vostri pagamenti, ordini di acquisto e informazioni di fatturazione.

6.2.2 2.2 Per comunicare con voi

Potremmo trattare i dati dei nostri clienti o dei loro singoli utenti finali, in particolare e-mail o altri dati di contatto, per comunicare con i nostri utenti e utenti finali, ad esempio quando li assistiamo nella configurazione o nell'amministrazione del loro account, quando forniamo assistenza e supporto ai clienti, inviamo avvisi tecnici, aggiornamenti su imminenti modifiche o miglioramenti ai Servizi, promemoria, avvisi di sicurezza e altri messaggi di supporto e amministrativi.

6.2.3 2.3 Per fornire una migliore esperienza utente

Potremmo trattare i tuoi dati personali per capire come utilizzi i nostri Servizi e quindi migliorare continuamente l'esperienza utente, oltre a fornire un'assistenza clienti senza soluzione di continuità. Potremmo trattare tali dati personali anche per migliorare e potenziare i nostri Servizi esistenti e sviluppare nuove offerte. Ciò include statistiche sui prodotti e sul mercato, ricerche e analisi, benchmark e altre analisi per comprendere meglio le tue esigenze e quelle degli utenti nel loro complesso, diagnosticare i problemi e analizzare le tendenze.

6.2.4 2.4 Per proteggere i nostri Servizi e difendere i nostri diritti o quelli di terzi

Trattiamo i dati personali dell'utente per garantire la sicurezza e l'affidabilità del Servizio. Ciò include l'individuazione, la prevenzione e la risposta a frodi, abusi, rischi per la sicurezza e problemi tecnici che potrebbero danneggiare MyQ, i nostri clienti e gli utenti finali.

Potremmo trattare alcuni dei dati specificati nella Sezione 1.1 quando richiesto dalla legge o per stabilire, esercitare o difendere i nostri diritti legali o, se necessario, proteggere i diritti e gli interessi di MyQ.

6.2.5 2.5 Per finalità di marketing e vendita

Potremmo trattare i dati di contatto delle persone di riferimento designate dall'utente o dai suoi utenti finali al fine di fornire informazioni relative alle nuove funzionalità dei Servizi e alle nuove offerte di prodotti. Per maggiori dettagli, consultare la Sezione 7 di seguito.

6.3 3. Base giuridica

Per le finalità specificate nelle sezioni 2.1 e 2.2, trattiamo i vostri dati personali sulla base del nostro contratto con voi (se siete nostri clienti diretti e persone fisiche) o sulla base del nostro legittimo interesse a fornire i nostri Servizi ai nostri clienti (qualora il nostro cliente sia la vostra azienda o organizzazione e voi siate un utente finale autorizzato designato dalla vostra azienda o organizzazione).

Per le finalità specificate nella Sezione 2.3, trattiamo i dati personali dell'utente sulla base del nostro legittimo interesse a sviluppare e migliorare i nostri Servizi.

Per le finalità specificate nella Sezione 2.4, trattiamo i tuoi dati personali sulla base del nostro legittimo interesse a proteggere e garantire i nostri diritti o rivendicazioni o i diritti dei nostri clienti o utenti.

Per le finalità specificate nella Sezione 2.5, trattiamo i vostri dati personali sulla base del vostro consenso volontario, qualora ci abbiate fornito tale consenso. In un ambito limitato consentito dalla legge applicabile, potremmo anche utilizzare i vostri recapiti elettronici per informarvi sui nostri Servizi senza il vostro consenso esplicito, sulla base del nostro legittimo interesse, come descritto più dettagliatamente nella Sezione 7 di seguito.

Quando utilizziamo i tuoi dati personali per i nostri legittimi interessi, ci assicuriamo di tenere conto di qualsiasi potenziale impatto che tale utilizzo potrebbe avere su di

te. I nostri interessi legittimi non prevalgono automaticamente sui tuoi e non utilizzeremo le tue informazioni se riteniamo che i tuoi interessi debbano prevalere sui nostri, a meno che non abbiamo altri motivi per farlo (come l'esecuzione di un contratto, il tuo consenso o un obbligo legale). Se hai dubbi sul nostro trattamento dei dati, consulta i dettagli della sezione "I tuoi diritti" nella Sezione 9 di seguito.

6.4 4. Periodi di conservazione

Quando trattiamo i dati personali in qualità di titolari del trattamento, conserviamo i dati personali dell'utente per il periodo necessario a soddisfare le finalità descritte nella presente Informativa sulla privacy e/o in qualsiasi contratto di servizi, a meno che la legge non richieda una conservazione più lunga (ad esempio per scopi fiscali o contabili o a causa di altri requisiti legali) o la conservazione dei dati sia necessaria per l'accertamento, l'esercizio o la difesa di diritti legali di MyQ; in tal caso, conserveremo solo i dati necessari per l'esecuzione delle nostre rivendicazioni o la nostra difesa per il periodo necessario nel caso specifico e non oltre i termini di prescrizione previsti dalla legge.

Quando trattiamo dati personali per conto dei nostri clienti in qualità di responsabili del trattamento, conserviamo tali dati per la durata del nostro contratto con tali clienti e li cancelliamo automaticamente in conformità con le nostre procedure di conservazione e backup entro 90 giorni dalla risoluzione del contratto, a meno che i clienti non ci chiedano di cancellarli prima.

6.5 5. Condivisione dei dati personali per scopi legali e commerciali

Possiamo utilizzare e/o divulgare a terzi (compresi enti governativi e autorità di contrasto, nostre affiliate, consulenti professionali e nostri fornitori o subappaltatori) informazioni che vi riguardano quando:

- Rispettiamo un procedimento legale;
- facciamo valere o difendiamo i diritti legali di MyQ e in relazione a una ristrutturazione aziendale come una fusione, un'acquisizione aziendale o situazioni di insolvenza;
- Prevenire frodi o danni imminenti; e
- Garantiamo la sicurezza e l'operatività della nostra rete e dei nostri servizi.

Tali informazioni saranno condivise a condizione che, in tutte queste circostanze, condivideremo solo le informazioni personali limitate che è necessario condividere nella situazione specifica.

Condividiamo i tuoi dati con i nostri partner commerciali di fiducia o con persone che trattano i tuoi dati in qualità di nostri responsabili del trattamento per nostro conto e secondo le nostre istruzioni, in conformità con la presente Informativa sulla privacy. Selezioniamo i nostri fornitori con molta attenzione e ci assicuriamo sempre che forniscano adeguate garanzie in materia di protezione dei dati e sicurezza. A tal fine, abbiamo vincolato i nostri responsabili del trattamento dei dati con accordi sul trattamento dei dati conclusi ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) ("GDPR").

Se si seleziona il tenant dei Servizi nell'interfaccia di amministrazione MyQ con sede nell'UE, i Dati del Cliente saranno trattati nell'UE, in conformità con gli impegni contrattuali di Microsoft relativi ai confini dei dati dell'UE. Se si seleziona il tenant dei Servizi nell'interfaccia di amministrazione MyQ con sede al di fuori dell'UE, tale trasferimento sarà effettuato sulla base delle Clausole Contrattuali Standard (clausole modello) approvate dalla Commissione Europea (2010/87/UE), a meno che non sia disponibile un meccanismo di trasferimento diverso ai sensi degli articoli 45, 46 e seguenti del GDPR. Fermo restando quanto sopra, i dati dei clienti potrebbero anche essere trasferiti in paesi per i quali la Commissione europea ha emesso una decisione di adeguatezza.

L'elenco dei nostri attuali responsabili del trattamento che potrebbero avere accesso ai dati personali dell'utente:

- http://salesforce.com EMEA Ltd. (elaborazione relativa alle vendite e assistenza tecnica),
- Microsoft Ireland Operations Limited (collaborazione e comunicazione, Microsoft Azure – servizi di cloud hosting),
- TeamViewer GmbH (assistenza tecnica).

Oltre ai responsabili del trattamento sopra menzionati, potremmo anche condividere i dati personali dell'utente per gestire i nostri processi aziendali e adempiere ai nostri obblighi legali, inclusi servizi logistici, di fatturazione, fiscali, legali e tecnici.

Oltre ai fornitori terzi, MyQ può condividere i dati con le sue affiliate situate nell'UE e nel Regno Unito per determinati servizi logistici, di fatturazione, fiscali, legali e tecnici. L'elenco aggiornato delle nostre affiliate nell'UE e nel Regno Unito è disponibile all'indirizzo https://www.myq-solution.com/en/the-list-of-myq-data-processors .

6.6 6. Statistiche anonime

Possiamo utilizzare dati aggregati e resi anonimi derivati dai dati personali forniti dall'utente o raccolti dall'analisi del programma, come il comportamento e le attività degli utenti, per le nostre statistiche, per la revisione contabile, per scopi di ricerca sui prodotti e sul mercato, per analisi (che ci aiutano a ottimizzare e migliorare i nostri Servizi e la loro usabilità, la gamma di Servizi e a sviluppare nuove tecnologie, prodotti e servizi) e per benchmark e altre analisi.

6.7 7. Comunicazioni di marketing

Potremmo contattare le persone di contatto designate dall'utente o dai suoi utenti finali al fine di fornire informazioni relative alle nuove funzionalità dei Servizi e alle nuove offerte di prodotti, a condizione che abbiamo il permesso necessario per farlo, sulla base del consenso dell'utente (ove lo abbiamo richiesto e l'utente ce lo ha fornito) o dei nostri legittimi interessi a fornire all'utente comunicazioni di marketing laddove possiamo farlo legalmente, nei limiti previsti dalla legge. In quest'ultimo caso, vi invieremo comunicazioni di marketing solo se state utilizzando o avete recentemente utilizzato uno dei nostri Servizi e non avete obiettato alla ricezione di tali informazioni (con uno dei mezzi indicati di seguito).

Le tue preferenze in materia di comunicazioni di marketing possono essere modificate in qualsiasi momento seguendo le istruzioni riportate di seguito:

- Se desideri annullare l'iscrizione a un'e-mail che ti è stata inviata, segui il link "annulla iscrizione" e/o le istruzioni riportate in fondo all'e-mail.
- In alternativa, puoi contattarci utilizzando i dettagli riportati nella sezione "Contattaci" qui sotto per modificare le tue preferenze in materia di comunicazioni di marketing, compreso il ritiro del tuo consenso.

Se hai ricevuto e-mail indesiderate e non richieste inviate tramite il nostro sistema o che sembrano essere state inviate tramite il nostro sistema, inoltra una copia di tale e-mail con i tuoi commenti a info@myq-solution.com[1] per la revisione.

Si prega di notare che occasionalmente potremmo inviare informazioni importanti (anche tramite e-mail) sui Servizi che l'utente sta utilizzando o ha utilizzato, comprese le modifiche ai termini e alle condizioni applicabili e/o altre comunicazioni o notifiche che potrebbero essere necessarie per adempiere ai nostri obblighi legali e contrattuali, come descritto nella Sezione 2.2 sopra. Queste importanti

1. mailto:info@myq-solution.com

comunicazioni relative al Servizio non costituiscono comunicazioni di marketing e non sono influenzate dalle preferenze dell'utente.

6.8 8. Sicurezza e ubicazione dei dati dell'utente

Abbiamo implementato e manterremo misure tecniche e organizzative adeguate, controlli interni e routine di sicurezza delle informazioni in conformità con le buone pratiche del settore, tenendo conto dello stato di sviluppo tecnologico, al fine di proteggere i tuoi dati da perdita accidentale, distruzione, alterazione, divulgazione o accesso non autorizzato o distruzione illegale. Tali misure possono includere, a titolo esemplificativo ma non esaustivo, l'adozione di misure ragionevoli per garantire l'affidabilità dei dipendenti che hanno accesso ai dati dell'utente e la previsione di diritti di accesso limitati e controlli di accesso; autenticazione; formazione del personale; backup regolari; procedure di recupero dei dati e di gestione degli incidenti; restrizioni alla conservazione, alla stampa e allo smaltimento dei dati personali; protezione software dei dispositivi su cui sono memorizzati i dati personali; ecc.

6.9 9. I vostri diritti

La presente Sezione descrive i diritti dell'utente ai sensi delle leggi applicabili, come il GDPR, e come esercitarli. Se l'utente esercita uno qualsiasi dei suoi diritti ai sensi della presente Sezione o delle leggi applicabili, comunicheremo qualsiasi rettifica o cancellazione dei suoi dati personali o restrizione del trattamento effettuata in conformità con la sua richiesta a ciascun destinatario a cui i dati personali sono stati comunicati ai sensi della Sezione 5 della presente Informativa sulla privacy, a meno che tale comunicazione non risulti impossibile o comporti uno sforzo sproporzionato.

Se desideri esercitare tali diritti e/o ottenere tutte le informazioni rilevanti sul trattamento dei tuoi dati personali, ti preghiamo di contattarci all'indirizzo info@myq-solution.com[2]. Ti verrà chiesto di identificarti; ciò è necessario per verificare che la richiesta sia stata inviata da te. Risponderemo entro 1 mese dal ricevimento della richiesta, ma ci riserviamo il diritto di prorogare tale termine fino a 2 mesi in circostanze eccezionali e giustificate. In ogni caso, vi informeremo entro 1 mese dal ricevimento della richiesta se decidiamo di prorogare il termine per la nostra risposta.

2. mailto:info@myq-solution.com

In conformità con le leggi applicabili e come descritto più dettagliatamente di seguito, hai il diritto di richiedere l'accesso ai tuoi dati personali e alle informazioni relative al loro trattamento, il diritto di rettifica, cancellazione o portabilità (ad esempio, trasferimento dei tuoi dati personali a un altro fornitore di servizi) dei tuoi dati personali che trattiamo, nonché il diritto di opporti al trattamento dei tuoi dati personali e/o richiedere la limitazione di tale trattamento.

Si prega di notare che la vostra opposizione al trattamento potrebbe comportare l'impossibilità da parte nostra di fornirvi i nostri Servizi o di eseguire le azioni necessarie per raggiungere gli scopi sopra indicati (vedere la Sezione 2 "Come utilizziamo i dati").

È importante che i dati personali in nostro possesso siano accurati e aggiornati. Ti preghiamo di tenerci informati se i tuoi dati personali cambiano durante il tuo rapporto con noi, contattandoci tramite i recapiti indicati nella Sezione 10 "Contattaci".

6.9.1 9.1 Informazioni sui dati personali dell'utente, accesso agli stessi e rettifica degli stessi

In base alle leggi applicabili, hai il diritto di ottenere la conferma che i tuoi dati personali siano o meno oggetto di trattamento (secondo la procedura sopra descritta) e, in tal caso, il diritto di accedere e rettificare i tuoi dati personali che hai condiviso con noi. Attraverso le impostazioni dei Servizi, puoi accedere e aggiornare le informazioni del tuo account e modificare le impostazioni del tuo profilo.

6.9.2 9.2 Accuratezza dei dati personali

Adottiamo misure ragionevoli per garantire che l'utente sia in grado di mantenere i propri dati personali accurati e aggiornati. L'utente può sempre contattarci per ottenere conferma del fatto che stiamo ancora trattando i suoi dati personali.

Se l'utente scopre che i suoi dati personali da noi trattati sono inesatti o incompleti e non è in grado di aggiornarli in conformità con la Sezione 9.1 della presente Informativa sulla privacy, può richiederci di aggiornare tali dati personali. Verificheremo l'identità dell'utente e aggiorneremo i suoi dati personali per suo conto.

6.9.3 9.3 Cancellazione dei dati personali

Puoi chiederci di cancellare i tuoi dati personali in qualsiasi momento. Se ci contatti con tale richiesta, cancelleremo tutti i tuoi dati personali in nostro possesso senza

indebito ritardo, a condizione che i tuoi dati personali non siano più necessari per la fornitura dei Servizi o per altri scopi consentiti, in particolare in relazione all'esercizio e alla difesa dei nostri diritti legali o all'adempimento dei nostri obblighi legali. Cancelleremo inoltre (e garantiremo la cancellazione da parte dei responsabili del trattamento da noi incaricati) tutti i tuoi dati personali nel caso in cui tu revochi il tuo consenso o nelle circostanze in cui la legge ci impone di farlo.

6.9.4 9.4 Limitazione del trattamento

Se ci richiedi di limitare il trattamento dei tuoi dati personali, ad esempio in circostanze in cui contesti l'accuratezza, la liceità o la nostra necessità di trattare i tuoi dati personali, limiteremo il trattamento dei tuoi dati personali al minimo necessario (archiviazione) e, se applicabile, li tratteremo solo per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o, se necessario, per la tutela dei diritti di un'altra persona fisica o giuridica, o per altri motivi limitati dettati dalla legge applicabile. Nel caso in cui la limitazione venga revocata e noi continuiamo a trattare i tuoi dati personali, sarai informato di conseguenza senza indebito ritardo.

6.9.5 9.5 Portabilità dei dati personali

Hai il diritto di ricevere i dati personali che ti riguardano e che ci hai fornito. Se ci invii una richiesta in tal senso, ti forniremo i tuoi dati personali in un formato comunemente utilizzato e leggibile da dispositivo automatico senza indebito ritardo dal ricevimento della tua richiesta. Se lo richiedi, invieremo i tuoi dati personali a una terza parte (un altro titolare del trattamento) che identificherai nella tua richiesta, a meno che tale richiesta non pregiudichi i diritti o le libertà di altri e ove tecnicamente fattibile.

6.9.6 9.6 Opposizione al trattamento

Hai il diritto di opporti al nostro utilizzo dei tuoi dati personali sulla base dei nostri legittimi interessi. In tal caso, non tratteremo più i tuoi dati personali a meno che non dimostriamo motivi legittimi convincenti per il loro ulteriore trattamento che prevalgano sui tuoi interessi, diritti e libertà, o per l'istituzione, l'esercizio o la difesa dei nostri diritti legali. Se ti opponi al trattamento dei tuoi dati per finalità di marketing diretto, cesseremo di trattare i tuoi dati per tali finalità.

6.9.7 9.7 Revoca del consenso

Se ci avete fornito il vostro consenso al trattamento dei dati personali, ad esempio per comunicazioni di marketing, potete revocare il vostro consenso in qualsiasi momento senza fornire alcuna motivazione. Bloccheremo i vostri dati personali per qualsiasi ulteriore trattamento. Si prega di notare che la revoca del vostro consenso non pregiudica la liceità di qualsiasi trattamento basato sul consenso prima della sua revoca.

6.9.8 9.8 Reclamo all'autorità garante della protezione dei dati

Hai il diritto di presentare un reclamo relativo alle nostre attività di trattamento dei dati all'Úřad pro ochranu osobních údajů, all'indirizzo Pplk. Sochora 2Z, 170 00 Praha 7, Repubblica Ceca.

6.9.9 9.9 Richiesta di rinuncia alla vendita dei dati personali ai sensi del CCPA

MyQ non vende, secondo la definizione del CCPA, alcun dato personale. Pertanto, se un consumatore californiano comunica una richiesta di rinuncia ai sensi di questa disposizione, essa non avrà alcun effetto. Se desiderate ulteriori informazioni sui vostri diritti ai sensi del CCPA di rinunciare alla vendita dei vostri dati personali, contattate: info@myq-solution.com[3].

6.10 10. Contattaci

Per qualsiasi domanda relativa alle nostre pratiche di raccolta e protezione dei dati o ai propri diritti, non esitare a contattarci all'indirizzo info@myq-solution.com[4].

3. mailto:info@myq-solution.com
4. mailto:info@myq-solution.com

7 Uptime del server, backup dei dati e disaster recovery

7.1 Tempo di attività del server

MyQ Roger si impegna a mantenere un obiettivo di uptime del 99,9%; tuttavia, gli accordi sul livello di servizio (SLA) sono personalizzati per ogni cliente e non garantiscono esplicitamente questo parametro. Utilizziamo strategie avanzate di alta disponibilità (HA), sfruttando implementazioni multizona e architetture multipod per garantire la continuità del servizio e ridurre al minimo i potenziali tempi di inattività in caso di interruzioni operative.

7.2 Monitoraggio dello stato del sistema in tempo reale

Per migliorare la trasparenza e fornire visibilità in tempo reale sulle prestazioni del sistema, manteniamo un sito dedicato allo stato che fornisce informazioni aggiornate sullo stato di salute del servizio. Questa piattaforma consente ai clienti di:

- **Monitorare lo stato del sistema in tempo reale**: visualizzare metriche operative in tempo reale e aggiornamenti sugli incidenti.
- **Ricevere notifiche proattive**: iscriversi agli avvisi relativi al degrado del servizio o agli eventi di manutenzione pianificata.
- **Accedere ai rapporti storici sull'uptime**: esaminare gli incidenti passati e le tendenze delle prestazioni per valutare l'affidabilità.

Offrendo un sito centralizzato dedicato allo stato del sistema, forniamo ai clienti informazioni tempestive e accurate, rafforzando la fiducia e consentendo un processo decisionale proattivo in caso di interruzioni.

7.3 Strategie di backup

7.3.1 Strategia di backup di Azure SQL

Utilizziamo una strategia di backup geo-ridondante per i database SQL di Azure, garantendo la resilienza e la recuperabilità dei dati. Gli aspetti chiave includono:

- **Archiviazione geo-ridondante**: i backup vengono replicati in più regioni per il ripristino di emergenza.
- **Politica di conservazione**: i backup vengono conservati per diversi mesi, consentendo il ripristino dei dati storici.
- **Backup incrementali**: una finestra di ripristino point-in-time (PITR) di 14 giorni consente il ripristino granulare dei dati persi.

- **Personalizzazione basata su SLA**: i periodi di conservazione e gli obiettivi di tempo di ripristino (RTO) variano in base agli SLA specifici del cluster e possono essere personalizzati per soddisfare le esigenze dei clienti.

7.3.2 Strategia di backup di Azure Cosmos DB

Per Azure Cosmos DB, implementiamo meccanismi completi di protezione dei dati, in particolare per i registri contabili, garantendo l'integrità e la tracciabilità dei dati:

- **Report completi dei dati contabili**: tutte le transazioni contabili, compresa la contabilità dei lavori di stampa, scansione, copia e fax, vengono registrate integralmente.
- **Ricostruzione dei dati storici**: il nostro sistema consente di tracciare e ricostruire qualsiasi registrazione contabile segnalata per garantire la conformità e la verificabilità.
- **Alta disponibilità e ridondanza**: la replica multiregionale integrata garantisce la continuità e riduce al minimo i rischi di perdita di dati.

Implementando queste solide strategie di backup, salvaguardiamo i dati aziendali critici, fornendo al contempo opzioni di ripristino flessibili su misura per gli SLA specifici dei clienti.

7.4 Scenari di emergenza e piano di risposta

Scenario di emergenza	Strategia di mitigazione	Processo di ripristino
Corruzione dei dati	PITR (ripristino a un punto nel tempo)	Ripristino del database all'ultimo stato corretto conosciuto
Interruzione della regione cloud	Backup georedondanti e failover	Passaggio alla regione Azure secondaria
Guasto del nodo Kubernetes	Replica automatica dei servizi in AKS	I pod vengono riprogrammati su nodi funzionanti
Attacchi informatici (DDoS, ransomware, ecc.)	WAF, protezione DDoS di Azure e monitoraggio della sicurezza	Isolamento dei sistemi compromessi, ripristino da backup puliti

8 Fiducia zero

8.1 Comprendere la sicurezza Zero Trust

La fiducia è un concetto complesso. Ad esempio, mi fido di mia madre quando cucina una cena perfetta, ma non mi fiderei mai di lei per la sicurezza della rete. Nella sicurezza informatica, una fiducia mal riposta può portare a vulnerabilità significative, ed è per questo che esiste il modello Zero Trust.

8.1.1 Esempio reale: il pericolo della fiducia implicita

Una delle violazioni più note in cui la mancanza dei principi Zero Trust ha avuto un ruolo importante è stato l'**attacco alla Colonial Pipeline** nel 2021. Gli aggressori hanno ottenuto l'accesso tramite credenziali VPN compromesse, che non avevano l'autenticazione a più fattori (MFA) abilitata. Poiché la rete si fidava implicitamente degli utenti autenticati, gli aggressori sono stati in grado di muoversi lateralmente e distribuire ransomware, causando una diffusa carenza di carburante in tutti gli Stati Uniti. Questo incidente evidenzia perché "non fidarsi mai, verificare sempre" è fondamentale per la sicurezza informatica moderna.

8.2 Che cos'è Zero Trust?

Zero Trust è un paradigma di sicurezza informatica basato sul principio "non fidarti mai, verifica sempre". Assicura che gli utenti e i dispositivi non siano considerati affidabili per impostazione predefinita, anche se sono collegati a una rete aziendale protetta o sono stati precedentemente verificati. Al contrario, l'affidabilità deve essere continuamente valutata e convalidata sulla base di vari segnali di sicurezza.

8.2.1 I principi fondamentali di Zero Trust

Zero Trust è definito nella norma **NIST SP 800-207** come un framework incentrato sulla protezione delle risorse attraverso la verifica continua. Questo modello di sicurezza si applica a:

- **Gestione delle identità e degli accessi**: garantire che gli utenti e i dispositivi si autenticino in modo sicuro.
- **Sicurezza della rete e degli endpoint**: protezione delle comunicazioni e applicazione di rigorosi controlli di accesso.
- **Protezione dei dati**: garantire che i dati sensibili siano crittografati e archiviati in modo sicuro.

- **Monitoraggio continuo**: rilevare anomalie e rispondere alle potenziali minacce in tempo reale.

8.3 Come Zero Trust si applica a MyQ Roger

8.3.1 Verifica esplicita

- L'autenticazione è richiesta anche sui dispositivi autorizzati (telefoni/desktop).
- Utilizza standard di autenticazione moderni.
- L'autenticazione a più fattori (MFA) è obbligatoria per gli accessi da dispositivi mobili e stampanti multifunzione (MFP).
- OAuth2 Device Flow è implementato per l'autorizzazione dei dispositivi.
- **I meccanismi di autenticazione continua** tracciano i cambiamenti nel comportamento degli utenti per rilevare eventuali anomalie.

8.3.2 Gestione degli accessi

- **Il controllo degli accessi basato sui ruoli (RBAC)** garantisce che gli utenti dispongano solo dell'accesso minimo necessario.
- **Il principio del privilegio minimo** viene applicato per ridurre i rischi per la sicurezza.
- **La microsegmentazione** è implementata per limitare i movimenti laterali all'interno della rete.
- **I controlli di accesso Just-in-Time (JIT)** regolano dinamicamente i privilegi degli utenti in base al contesto.

8.3.3 Sicurezza dei dispositivi e degli endpoint

- Vengono emessi token di accesso univoci per ogni tipo di dispositivo.
- Il protocollo TLS (Transport Layer Security) è obbligatorio per tutte le comunicazioni.
- **Le soluzioni EDR (Endpoint Detection and Response)** monitorano e analizzano il comportamento dei dispositivi.
- **Zero Trust Network Access (ZTNA)** garantisce che solo i dispositivi autorizzati possano accedere a risorse specifiche.

8.3.4 Protezione dei dati

- Tutti i dati vengono archiviati in modo sicuro utilizzando soluzioni di archiviazione crittografate.
- Le politiche garantiscono che i dati siano accessibili solo da entità autorizzate.
- **Le soluzioni DLP (Data Loss Prevention)** monitorano e impediscono l'esfiltrazione non autorizzata dei dati.

- **Le enclavi sicure** proteggono i dati altamente sensibili da accessi non autorizzati.

8.4 Affrontare le minacce informatiche con Zero Trust

Zero Trust aiuta a mitigare le seguenti minacce:

- **Minacce interne**: impedisce ai dipendenti o agli account compromessi di ottenere un accesso non autorizzato.
- **Attacchi di credential stuffing e phishing**: riduce l'impatto delle credenziali compromesse attraverso l'autenticazione continua.
- **Attacchi di movimento laterale**: la microsegmentazione impedisce agli aggressori di muoversi lateralmente attraverso le reti.
- **Attacchi alla catena di fornitura**: garantisce una verifica rigorosa dell'accesso e delle integrazioni di terze parti.

8.5 Considerazioni relative alla conformità e alle normative

Zero Trust è in linea con varie normative e framework di sicurezza informatica:

- **ISO 27001**: impone una gestione sicura degli accessi e la protezione dei dati.
- **GDPR**: garantisce l'elaborazione e l'archiviazione sicura dei dati personali.
- **HIPAA**: protegge le informazioni sanitarie sensibili.
- **NIST Cybersecurity Framework**: fornisce linee guida per l'implementazione di Zero Trust.

8.6 Perché Zero Trust è importante

L'adozione dello Zero Trust riduce al minimo il rischio di violazioni della sicurezza, minacce interne e accessi non autorizzati. In un'epoca di crescenti minacce informatiche, un'architettura Zero Trust fornisce una protezione robusta garantendo una verifica continua e controlli di accesso rigorosi su tutte le risorse.

Attraverso l'implementazione di questi principi, MyQ Roger garantisce un approccio alla sicurezza sicuro, resiliente e adattivo, in linea con le migliori pratiche moderne in materia di sicurezza informatica. Inoltre, il monitoraggio continuo, i controlli di accesso e il rilevamento delle minacce in tempo reale migliorano la capacità dell'organizzazione di rispondere in modo efficace alle minacce informatiche in continua evoluzione.

9 Accesso sicuro con MyQ Roger

9.1 Introduzione

L'utilizzo di un PIN come metodo principale di accesso non è mai stato veramente sicuro. I primi telefoni cellulari si basavano sui PIN, ma con l'evolversi delle preoccupazioni in materia di sicurezza, anche i metodi di autenticazione si sono evoluti. Oggi la biometria è diventata la norma, offrendo un approccio più sicuro e intuitivo all'autenticazione.

MyQ Roger abbraccia questo cambiamento implementando l'ultima versione di OAuth 2.0 Device Authorization Grant (precedentemente noto come Device Flow). Questo moderno metodo di autenticazione richiede agli utenti di accedere utilizzando un codice QR monouso scansionato con il proprio telefono cellulare, eliminando la necessità di password statiche o PIN non sicuri.

Riconosciamo il cellulare di un utente come uno dei mezzi di autenticazione più sicuri. Sfruttando l'autenticazione biometrica per sbloccare il telefono e successivamente accedere all'app MyQ, garantiamo che la persona che effettua l'accesso sia il legittimo proprietario dell'account.

9.2 Autenticazione sicura con MyQ Roger

- **OAuth 2.0 Device Authorization Grant**: invece di affidarsi ai tradizionali PIN, gli utenti si autenticano utilizzando un codice QR generato dinamicamente. Questo metodo riduce significativamente il rischio di furto delle credenziali o di attacchi di riutilizzo.
- **Verifica biometrica**: poiché gli smartphone moderni richiedono la verifica biometrica (ad esempio, impronta digitale o riconoscimento facciale) per sbloccarsi, ciò aggiunge un ulteriore livello di sicurezza prima di accedere a MyQ Roger.

9.3 Autenticazione con PIN legacy

Sebbene MyQ Roger continui a offrire il login basato su PIN come opzione, questo metodo è considerato poco sicuro e sconsigliato per impostazione predefinita. Gli utenti che scelgono di abilitare l'autenticazione tramite PIN devono contrassegnarla esplicitamente come sicura, riconoscendo i rischi per la sicurezza associati. Inoltre, l'abilitazione del login tramite PIN disattiverà alcune funzionalità di sicurezza avanzate per mitigare potenziali vulnerabilità.

9.4 Responsabilità in materia di sicurezza

Se un'organizzazione decide di consentire l'accesso tramite PIN, la responsabilità di mantenere un ambiente sicuro ricade sul cliente. Per ridurre al minimo i rischi, è necessario seguire le migliori pratiche, come l'applicazione di politiche rigorose in materia di PIN, l'implementazione di misure di sicurezza fisica e il monitoraggio dei registri di accesso.

9.5 Conclusione

Con MyQ Roger, diamo priorità alla sicurezza sfruttando i moderni standard di autenticazione. L'adozione dell'autenticazione biometrica basata su dispositivi mobili garantisce un'esperienza utente fluida ma sicura. Sebbene l'accesso basato su PIN legacy rimanga disponibile, non è il metodo consigliato e i clienti devono prendere ulteriori precauzioni se scelgono di utilizzarlo. Adottando meccanismi di accesso sicuri, le organizzazioni possono migliorare sia la sicurezza che l'usabilità per i propri utenti.

10 Stampa sicura con MyQ Roger

10.1 La sfida della stampa sicura

I metodi tradizionali di stampa sicura si basano su connessioni fisicamente collegate, come i cavi LPT, in cui una stampante dedicata è assegnata a un singolo laptop. Sebbene questo metodo garantisca il massimo livello di sicurezza, è poco pratico negli ambienti moderni che richiedono flessibilità, mobilità e risorse condivise.

AirPrint e Mopria offrono funzionalità di stampa sicura, ma sono insufficienti in scenari in cui gli utenti possono avviare lavori di stampa remoti senza essere fisicamente presenti vicino alla stampante. Ciò crea vulnerabilità di sicurezza in cui documenti sensibili potrebbero essere lasciati incustoditi.

10.2 MyQ Roger: una soluzione completa per la stampa sicura

MyQ Roger integra più flussi di lavoro di stampa applicando protocolli di sicurezza per garantire che gli utenti debbano essere fisicamente presenti per autenticarsi e rilasciare i lavori di stampa. Il sistema garantisce che i lavori di stampa siano archiviati e trasmessi in modo sicuro, riducendo al minimo l'esposizione dei dati.

10.3 Metodi di stampa sicuri in MyQ Roger

10.3.1 1) Stampa diretta da PC a stampante

- Utilizza **IPP/s (Internet Printing Protocol Secure)** per trasferire i lavori di stampa in modo sicuro.
- Marche di stampanti supportate: **Ricoh, Kyocera**.
- I lavori di stampa rimangono memorizzati direttamente sulla stampante fino a quando l'utente non li autentica e li rilascia.

10.3.2 2) MyQ Roger Client (MRC)

- I lavori di stampa vengono **crittografati e memorizzati localmente** sul PC dell'utente.
- La stampante recupera il file crittografato **solo dopo l'autenticazione dell'utente**.
- La stampa sicura viene eseguita tramite **IPP/s**.

10.3.3 3) Stampa cloud

- I file di stampa vengono archiviati in modo sicuro nel cloud storage dell'utente (ad esempio **OneDrive**, **Google Drive, Dropbox**).

- La stampante scarica il documento direttamente dall'archivio cloud utilizzando un **link di accesso a breve durata**.
- **Nessun documento viene conservato** sulla stampante dopo la stampa, garantendo la riservatezza dei dati.

10.3.4 4) Integrazione con Microsoft Universal Print

- MyQ Roger implementa un **connettore Universal Print** che consente alle stampanti di comunicare direttamente con **i server Universal Print di Microsoft**.
- I lavori di stampa vengono archiviati in modo sicuro sui **server Microsoft** e recuperati su richiesta dopo l'autenticazione dell'utente.
- La stampa viene eseguita tramite **driver Universal Print**, garantendo una gestione dei lavori fluida e sicura.

10.4 Conclusione

MyQ Roger offre un **ambiente di stampa olistico e sicuro** combinando flussi di lavoro di stampa diretti, locali e basati su cloud con solide misure di sicurezza. Richiedendo agli utenti di autenticarsi di persona prima dell'esecuzione del lavoro, MyQ Roger elimina i rischi associati ai lavori di stampa incustoditi, garantendo la massima protezione dei dati nei moderni ambienti di lavoro.

11 Contatti commerciali

Produttore MyQ®	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Praga 9, Repubblica Ceca Numero identificativo 615 06 133 MyQ® spol. s r.o. è iscritta nel Registro delle Imprese presso il Tribunale Municipale di Praga, numero di registrazione C 29842 (di seguito denominata "MyQ®")
Informazioni commerciali	http://www.myq-solution.com info@myq-solution.com[5]
Assistenza tecnica	support@myq-solution.com[6]
Avviso	IL PRODUTTORE NON SARÀ RESPONSABILE DI EVENTUALI PERDITE O DANNI CAUSATI DALL'INSTALLAZIONE O DAL FUNZIONAMENTO DEL SOFTWARE E DELLE PARTI HARDWARE DELLA SOLUZIONE DI STAMPA MyQ®. Il presente manuale, il suo contenuto, il suo design e la sua struttura sono protetti da copyright. La copia o altra riproduzione totale o parziale della presente guida, o di qualsiasi oggetto protetto da copyright, senza il previo consenso scritto di MyQ® è vietata e può essere punibile. MyQ® non è responsabile del contenuto del presente manuale, in particolare per quanto riguarda la sua integrità, attualità e occupazione commerciale. Tutto il materiale qui pubblicato ha esclusivamente carattere informativo. Il presente manuale è soggetto a modifiche senza preavviso. MyQ® non è tenuta ad apportare tali modifiche periodicamente né ad annunciarle, e non è responsabile della compatibilità delle informazioni attualmente pubblicate con l'ultima versione della soluzione di stampa MyQ®.

5. mailto:info@myq-solution.com
6. mailto:support@myq-solution.com

Marchi commerciali	"MyQ®", compresi i relativi loghi, è un marchio registrato di MyQ®. È vietato qualsiasi utilizzo dei marchi commerciali di MyQ®, compresi i relativi loghi, senza il previo consenso scritto di MyQ® Company. Il marchio commerciale e il nome del prodotto sono protetti da MyQ® e/o dalle sue affiliate locali.

RISPARMIA TEMPO CON SOLUZIONI DI STAMPA PERSONALIZZATE

info@myq-solution.com

myq-solution.com

MyQ Roger è una soluzione cloud-native progettata per gli uffici moderni cloud-first, che semplifica i flussi di lavoro documentali e consente navigazione, stampa e scansione sicure ovunque si trovino gli utenti.

50+ milioni
Utenti che si affidano a MyQ

1+ milione
Dispositivi attivi

26+
Marchi supportati

1000+
Partner certificati

Presente in **140+** paesi

Premi e certificazioni

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001