MyQ Roger Data Security Whitepaper 2.x

Generated from docs.myq-solution.com
August/2026

ENGLISH

Table of Contents

1 Introduction

The purpose of this document is to inform the customers of MyQ Roger about processes that involve establishing connections in the system and about security measures taken to protect consequent data transfer.

2 Glossary

- **IPP/s (Internet Printing Protocol over Secure TLS)**:
  - MyQ Roger ensures secure printing by utilizing the Internet Printing Protocol (IPP) over a TLS-encrypted channel, preventing unauthorized access and ensuring data integrity in transit.
  - MyQ Roger optimizes network traffic through efficient packet handling, reducing unnecessary data transmission and ensuring secure communication between endpoints.
- **TLS (Transport Layer Security)**:
  MyQ Roger enforces TLS 1.2/1.3 for secure data encryption in all communications, ensuring protection against interception and man-in-the-middle (MITM) attacks.
- **Data at Rest, Data in Transit**:
  - **Data at Rest**: MyQ Roger encrypts stored data using AES-256, ensuring that sensitive information remains secure against unauthorized access.
  - **Data in Transit**: All data transferred between clients, servers, and cloud services is encrypted using TLS to maintain integrity and confidentiality.
- **Zero Trust Infrastructure**:
  MyQ Roger follows a **Zero Trust** security model by implementing continuous authentication, device verification, and least privilege access for users and services.
- **IAM (Identity and Access Management)**:
  MyQ Roger integrates IAM best practices by enforcing secure user authentication, multi-factor authentication (MFA), and identity-based access controls.
- **RBAC (Role-Based Access Control)**:
  MyQ Roger implements RBAC to restrict permissions based on user roles, ensuring that only authorized personnel can access critical functions and sensitive data.
- **SSO (Single Sign-On)**:
  MyQ Roger supports **SSO** via OAuth2 integration, enabling seamless authentication across enterprise applications while maintaining security and compliance.

3 Operations Security

3.1 Introduction

Security is a top priority at MyQ Roger. We enforce a **security-first** approach at every stage of development, deployment, and operations. Given the critical nature of cloud environments, security must be **proactive, automated, and continuously monitored** to prevent breaches and unauthorized access.

Our **Secure Operations strategy** integrates **continuous monitoring, vulnerability management, infrastructure security, and compliance** to ensure the integrity of applications and infrastructure.

3.2 Monitoring

Continuous monitoring is essential for detecting and responding to threats in real time. MyQ implements a **multi-layered monitoring approach:**

3.2.1 Endpoint Detection and Response (EDR)

- Monitors all endpoints (servers, VMs, and containers) for suspicious activity.
- Uses **behavioral analytics and threat intelligence** to detect advanced threats.
- Automatically isolates compromised endpoints to prevent lateral movement.

3.2.2 Azure Defender (Now Defender for Cloud)

- Protects **Azure AKS, SQL Server, Virtual Machines, and Storage**.
- Provides **real-time threat detection** and security configuration recommendations.
- Integrates with **Microsoft Sentinel (SIEM)** for centralized alerting.

3.2.3 Host Scanning

- Scans **VMs, cloud instances, and on-premises servers** for misconfigurations and outdated software.
- Detects **privilege escalation risks, unauthorized access points, and outdated dependencies**.

3.2.4 Log Collection & Analysis

- **Centralized logging** on a separate cluster for scalability and isolation.
- **Logs from Kubernetes, applications, and infrastructure** are labeled for efficient retrieval.
- **Long-term retention policies** ensure compliance and security analysis.

- **Alerting mechanisms** detect anomalies and security incidents, integrating with SIEM.
- **Real-time log correlation** for API requests, authentication events, database queries, and firewall traffic.

3.2.5 Port Scanning

- Detects unauthorized **open ports** that expose services to threats.
- Uses **automated tools like Nmap and ZMap** to scan for **unexpected port changes**.

3.2.6 Container Scanning

- **Static and dynamic scanning** of Docker containers before deployment.
- Identifies vulnerabilities in **base images, application layers, and runtime permissions**.
- Integrated with **Trivy** for **image security scanning**.

3.2.7 Kubernetes Monitoring

- Uses **Azure Kubernetes Service (AKS) built-in monitoring** with **Prometheus & Grafana**.
- Monitors **Kubernetes API calls, RBAC policies, and pod security**.
- Alerts on **container privilege escalations, excessive resource usage, and lateral movement attempts**.

3.2.8 Regular TLS Scans

- MyQ performs **TLS security scans using Qualys SSL Labs** to ensure best practices.
- TLS configurations are evaluated to maintain an **A+ security rating**, mitigating risks from weak protocols.
- Automated tools verify **certificate validity, expiration tracking, and protocol strength**.

3.3 Vulnerability Management

3.3.1 Vulnerability Scanning

- **Regular scans** detect security flaws in applications and infrastructure.
- Includes **automated CVE scanning** for cloud-deployed components.
- Integrates with **DefectDojo, SonarQube, and Trivy** for risk assessment.

3.3.2 Penetration Testing

- Conducted regularly to identify security weaknesses before exploitation.
- Combines **automated and manual testing methodologies** for comprehensive assessment.
- Findings are **documented, prioritized, and remediated** accordingly.

3.4 Infrastructure Security

A **hardened infrastructure** ensures security beyond just monitoring. MyQ employs:

3.4.1 SIEM (Security Information and Event Management)

- **Microsoft Sentinel SIEM** collect security events for real-time detection.
- Analyzes logs from **firewalls, identity systems, application logs, audit logs, and threat feeds**.
- Enables **automated responses to detected threats**.

3.4.2 Security Tracking & Management

- **Jira Bug Database** tracks, categorizes, and prioritizes security vulnerabilities.
- **DefectDojo** consolidates test results, ensuring structured tracking of security engagements.
- Regular **patching and remediation** maintain a strong security posture.

3.4.3 Identity and Access Management (IAM)

- Enforces **Zero Trust** with **role-based access control (RBAC) and multi-factor authentication (MFA)**.
- Uses **Azure AD** for identity governance.
- **Privilege escalation alerts** detect unauthorized admin access.

3.5 Development Workflow

Secure software development is a critical aspect of MyQ's security strategy. The following measures ensure the integrity of code, pipelines, and cloud environments:

3.5.1 Secure Development Environment

- MyQ developers use **security-hardened environments** with endpoint protection.
- Developers must follow **secure coding practices and regular security training**.

3.5.2 GitLab Secure Pipelines

- GitLab CI/CD pipelines include **automated security checks, code reviews, and testing**.
- **Static Application Security Testing (SAST)** and **Dynamic Application Security Testing (DAST)** detect vulnerabilities.
- **Container Image Signing** ensures only trusted images are deployed.

3.5.3 IAM & Access Control

- Only **Selected DevOps and SecOps personnel** have access to Azure cloud environments.
- **Role-based access control (RBAC) with Just-In-Time (JIT) least privilege elevation** is enforced.

3.5.4 Azure Kubernetes & Container Security

- MyQ's **AKS clusters pull images only from Azure Container Registry (ACR)**.
- AKS environments enforce **network policies and Pod Security Standards (PSS)** to isolate workloads.

3.5.5 Secrets Management

- **All secrets and API keys are stored in Azure Key Vault**, accessible only to IAM-authorized personnel.
- **Trivy filesystem scans** are conducted before committing to Git to detect and prevent sensitive secrets.

3.6 Conclusion

MyQ's **Secure Operations strategy** is built on a foundation of **continuous monitoring, proactive threat management, and strong infrastructure security**. By leveraging **advanced security tools, strict access controls, and automated testing**, MyQ ensures a **secure, resilient cloud environment**.

With the **integration of TLS security scans, penetration testing, and centralized logging**, MyQ enhances its ability to **detect, respond to, and mitigate security risks** effectively.

Security is an **evolving challenge**, and MyQ remains committed to **enhancing security measures through regular updates, compliance audits, and security best practices**. By maintaining a **security-first mindset**, MyQ upholds the **integrity and confidentiality** of its services, ensuring **trust and reliability** for all stakeholders.

4 Applications Security

4.1 The Evolution of Security Threats

In the early days, before the internet was widespread, printers were directly connected via LPT cables, and security concerns were minimal. The biggest risk was physical—someone looking over a user's shoulder to see printed documents. The security landscape was straightforward, and cyber threats were virtually nonexistent.

However, as printers and devices became network-connected, the threat landscape changed drastically. With printers now accessible over local area networks (LANs) and even the internet, attackers no longer need physical access. Threats such as man-in-the-middle (MITM) attacks, unauthorized data interception, and remote exploits have become prevalent. Cybercriminals have evolved from looking over shoulders to eavesdropping on network traffic and exploiting vulnerabilities.

Mitigating these risks is a continuous challenge, as new threats emerge frequently. To address these evolving security challenges, MyQ Roger implements continuous security practices, proactive monitoring, and strong defense mechanisms.

4.2 MyQ Roger's Security Approach

MyQ Roger is built with a security-first approach, ensuring that innovation and user experience are always aligned with the highest security standards. Our commitment to security is reflected in our continuous efforts to integrate robust security measures at every stage of development. We adopt a "secure-by-default" philosophy, embedding security within our products and services from the ground up.

To achieve this, MyQ Roger leverages automation, data-driven risk assessments, and best-in-class security practices to proactively identify and mitigate threats. By implementing security controls early in the development cycle, following a **shift-left approach**, we ensure vulnerabilities are detected and remediated before they reach production. This proactive integration allows us to scale efficiently, reduce risks, and minimize security threats. Our approach reinforces our dedication to safeguarding customer data, workflows, and overall security posture.

4.3 Shifting Left in Security

Shifting security left means integrating security early in the software development lifecycle (SDLC) rather than addressing vulnerabilities later. By catching security issues in the initial development stages, we prevent costly fixes and mitigate

potential breaches. This proactive strategy ensures that every line of code meets the highest security standards before it reaches production, reducing risks and strengthening our overall security posture.

4.4 MyQ Security Responsibilities

MyQ Roger is committed to safeguarding customer data and ensuring a secure operational environment. Our core security responsibilities include:

- **Data Protection**: MyQ ensures customer data is securely stored and encrypted, preventing unauthorized access and ensuring data confidentiality.
- **Regular Security Patching**: We proactively apply security patches and updates to all systems to eliminate vulnerabilities before they can be exploited.
- **Access Control Management**: We enforce strict access policies following the principle of least privilege, ensuring that only authorized personnel can access sensitive resources.

By upholding these security principles, MyQ Roger fosters a culture of security, protecting users from potential threats while ensuring compliance with industry standards.

4.5 MyQ Roger Security Control/Management

While we rely on secure cloud infrastructure, MyQ Roger takes direct responsibility for implementing additional security layers and adhering to industry best practices. Our approach includes:

- **Key Management with Azure Key Vault**: We utilize Azure Key Vault to store and manage all secrets, private keys, and certificates securely, ensuring strict access controls and encryption.
- **ISO 27001 Certification**: We adhere to ISO 27001 standards to maintain a structured and consistent approach to information security.
- **Endpoint Detection and Response (EDR)**: We leverage advanced EDR solutions to detect, analyze, and mitigate security threats in real time, reducing response time and minimizing risks.
- **Secure Development Practices**: Our secure software development lifecycle includes vulnerability assessments, continuous monitoring, and automated security scans to detect and fix security flaws.
- **Regular Security Audits**: We conduct both internal and third-party audits to ensure compliance and proactively address security risks.
- **SIEM with Azure Sentinel**: We use Azure Sentinel for real-time threat detection, automated response, and continuous security monitoring across all cloud and network environments.

By implementing these security measures, MyQ Roger strengthens its overall security framework, ensuring that customer data remains protected at all times.

4.6 Microsoft Azure and Compliance

MyQ Roger runs on Microsoft Azure, leveraging Azure Kubernetes Service (AKS), Azure SQL Servers, and Azure Cosmos DB for MongoDB. By operating within Azure's infrastructure, we benefit from Microsoft's industry-leading security, compliance, and reliability standards.

4.6.1 Microsoft's Security and Compliance Responsibilities

- Azure adheres to global compliance frameworks such as ISO 27001, SOC 2, and GDPR in the EU, ensuring adherence to strict regulatory standards.
- Microsoft provides built-in security features such as network isolation, identity protection, and continuous threat detection, reducing attack surfaces.
- Azure services undergo rigorous security assessments and penetration testing to proactively identify and remediate vulnerabilities.

By leveraging Azure’s secure infrastructure, MyQ Roger adds its own security layers to create a robust and resilient security model that protects customer applications and data.

4.7 Customer Security Responsibilities

While MyQ Roger provides a secure infrastructure and best-in-class security measures, customers also have key responsibilities to ensure the security of their environment. These include:

- **Maintaining an Active User List**: Customers should continuously manage user access by leveraging automated user synchronization or manually disabling inactive accounts to minimize risk.
- **Role-Based Access Control (RBAC) Enforcement**: Customers must apply RBAC principles to restrict user access to only necessary permissions, ensuring stronger security and operational efficiency.
- **Securing the Local Network**: Even though MyQ Roger operates with a zero-trust model, customers should ensure that their local network adheres to best security practices, such as firewall configurations, network segmentation, and endpoint protection.
- **Proper Resource Maintenance**: All connected devices, including printers and multifunction devices (MFPs), should be regularly updated with the latest firmware and security patches to prevent vulnerabilities.

By adhering to these responsibilities, customers strengthen their security posture while benefiting from MyQ Roger's comprehensive security framework.

4.8 Security Automation

To further enhance security across the development lifecycle, MyQ Roger integrates automated security testing and external security assessments:

- **SAST (Static Application Security Testing)**: Conducted on every commit to detect security vulnerabilities early in the development cycle, reducing the likelihood of insecure code reaching production.
- **DAST (Dynamic Application Security Testing)**: Performed in sandbox environments to identify and mitigate runtime security risks before deployment.
- **External Penetration Testing**: We engage independent security experts to perform penetration testing, ensuring that our security defenses can withstand real-world attack scenarios.

By automating security testing and conducting regular external assessments, MyQ Roger maintains a proactive and resilient security posture.

4.9 Conclusion

At MyQ Roger, security is not an afterthought—it is an integral part of our product and development lifecycle. By combining secure-by-design principles, industry best practices, and a strong compliance framework, we provide a robust security posture that protects our customers' data and operations. Our commitment to continuous security improvements ensures that MyQ Roger remains resilient against evolving threats while maintaining the highest standards of reliability and trust. We will continue to evolve our security strategy, adapting to new challenges and leveraging the latest technologies to uphold our mission of providing a secure and seamless user experience.

5 Data Protection

5.1 Overview

Data protection is at the core of **MyQ Roger's** approach to security, ensuring that every aspect of its cloud-based printing and scanning solution adheres to the highest industry standards. A fundamental principle of MyQ Roger is that **no print or scan job data is ever transferred through its servers**. Instead, MyQ Roger strictly limits its data collection to essential **metadata**, such as **job file names, file sizes, and page count information**. This ensures operational efficiency while safeguarding user privacy.

5.2 Multi-Tenant Cloud Security

As a **multi-tenant cloud product**, MyQ Roger provides customers with an environment that is **logically isolated** to prevent cross-tenant data exposure.

To provide resilience, MyQ Roger relies on **Azure SQL** and **Azure Cosmos DB**, both of which offer built-in security features such as **data encryption at rest and in transit, automated threat detection, and access monitoring**. The cloud infrastructure undergoes continuous security assessments to mitigate risks associated with multi-tenant environments.

5.3 Encryption & Secure Communication

Security is embedded at every level of MyQ Roger’s operations. All communication between clients, cloud services, and printers is **encrypted using TLS (Transport Layer Security)** to prevent unauthorized access or tampering.

To further strengthen security, **publicly trusted Certificate Authorities (CAs)** sign all certificates used within MyQ Roger, ensuring the highest level of trust. Additionally, certificates are **rotated every three months**, reducing the risk of potential compromise and maintaining compliance with security best practices.

5.4 Compliance & Identity Management

MyQ Roger aligns with internationally recognized security standards, holding **ISO 27001 certification**, which demonstrates its commitment to implementing robust information security management practices.

To enforce strict access controls, **Role-Based Access Control (RBAC)** is implemented, ensuring that users are granted **only the permissions necessary for**

their role. This minimizes exposure to sensitive data and reduces the risk of accidental or intentional misuse.

5.5 GDPR Compliance

Ensuring compliance with the **General Data Protection Regulation (GDPR)** is a top priority for MyQ Roger. In accordance with GDPR principles, MyQ Roger follows stringent data protection measures to safeguard user privacy:

- **Data Minimization**: Only essential metadata is collected, eliminating the risk of storing sensitive user documents.
- **User Rights & Control**: Users have the ability to request **access, correction, deletion, or anonymization** of their personal data, as mandated by GDPR.
- **Transparency in Data Processing**: Clear and concise privacy policies outline how metadata is handled, stored, and protected.
- **Secure Data Storage**: All data is **encrypted at rest and in transit**, ensuring full compliance with GDPR's strict security requirements.
- **Anonymization Measures**: When required, MyQ Roger implements **data anonymization techniques** to ensure that personal data can no longer be attributed to a specific user, reinforcing privacy protection.

These measures ensure that MyQ Roger fully aligns with GDPR's core requirements, giving users control over their personal data while maintaining a secure and compliant environment.

5.6 Data Backups

To protect against data loss and ensure service reliability, MyQ Roger implements a **comprehensive data backup strategy**. This includes:

- **Automated Backups**: Regularly scheduled **incremental and full backups** ensure that data remains recoverable in the event of an incident.
- **Secure Storage**: Backups are encrypted using **AES-256 encryption**, ensuring that even in the unlikely event of unauthorized access, data remains unreadable.
- **Retention Policies**: Backups are **stored for a defined period** in alignment with compliance requirements, allowing for efficient recovery in case of system failure or disaster recovery scenarios.
- **Integrity Testing & Verification**: Regular **backup integrity tests** are conducted to confirm that stored backups are functional and reliable, ensuring seamless data restoration when needed.

By implementing these robust security, compliance, and backup measures, **MyQ Roger provides a secure, private, and highly efficient cloud-based printing and scanning solution** that meets the highest data protection standards in the industry.

6 Privacy Policy

Your privacy is our concern, and we are serious about it. This Privacy Policy for MyQ Roger Solution (the “Privacy Policy”) explains what type of information MyQ may collect, hold and process in connection with provision of any products, services, content, applications, or other components that form part of the MyQ Roger Solution (the “Services”), and how that information is used and protected. It also sets out how you can contact us if you have any queries or concerns regarding your personal data.

This Privacy Policy is issued by MyQ, spol. s.r.o., with its registered office at Harfa Business Center, Ceskomoravska 2532/19b, Prague, 19000, Czech Republic, company ID No. 615 06 133, registered in the Commercial Register held by the Municipal Court in Prague, section C, insert 29842 (“MyQ” or “us”).

We reserve the right to make changes to this Privacy Policy at any time. Please check the Privacy Policy periodically for changes, although, if you are our customer, we may also notify you via email of any changes that, in our sole discretion, materially impact your use of the Services or the way we process your personal data. Your continued use of our Services covered by this Privacy Policy will signify your acceptance of any and all changes to this Privacy Policy made by us from time to time.

6.1 1. Data we collect or receive

We collect personal data from our customers, as the users of the Services, and their end-users (which includes employees of our customers) in order to set up and manage user accounts and provide and administer the Services. We also collect usage data and metrics. We are the data controller in respect of this personal data.

With respect to personal data that may be included in the metadata of the Content, as defined in the Terms of Service https://www.myq-solution.com/en/myq-legal-documents , that the users or end-users manage using the Services, or with respect to the personal data that we may have access to while providing remote or local support services (the “Customer Data”), we process such personal data on behalf of our customers as a data processor. When we process the Customer Data to deliver the Services to our customers, we act in accordance with the instructions of our customers as their data processor. We always keep Customer Data that we process on behalf of our customers and pursuant to their instructions separate from our other customers’ data and keep them strictly confidential.

6.1.1 1.1 Data of users and end-users of our Services

We collect your personal data when:

- You create an account within our Services;
- You log into our Service, by entering your username (email) and password;
- You use our Services or otherwise interact with MyQ, for example when you submit any queries to us;
- You otherwise voluntarily provide such data to MyQ.

When you create an account with MyQ, we will ask you to complete a registration form indicating your first name, surname, email, company, and job title. You can also choose to add a phone number to your account.

We also collect and process your username (email) and password.

For purposes of analysis and improvement of our Services, our servers may automatically record information when you visit our website or use some of our Services ("usage data"), including:

- Information about third-party services that the user and its end-users connect to the Services for authentication purposes and connection to the user's cloud storage;
- Information about the user's devices, e.g., type and brand of the printers and their serial number;
- Information about the use of our Services, e.g., the amount of printed or scanned documents.

The Services enable you to connect to third-party applications or other services, e.g., One Drive or Google Disk, for the purpose of sharing documents and other Content with the Services. If you choose to connect to third-party services, we will ask for your permission to enable the Services to access such third-party services, however, MyQ will not process any personal data stored there, except for the Customer Data, as defined above.

If our Services are purchased by an entity, it is the individual users within such entity's organization who log into our Services platform and whose personal data are collected, as described above. Where such entity provides us directly with any personal data of its employees or other individual users that it authorized to access the Services, it must have all necessary consents, permissions or registrations to process and to provide to us its employees' or users' personal data.

6.1.2 1.2 Customer Data

To deliver our Services to our users and end-users, we may also process Customer Data, as defined above. The processing of Customer Data is subject to the users' privacy policy, and the users are obliged to ensure that the processing of such data is lawful and compliant with the applicable law. The data processing with respect to Customer Data performed by MyQ is regulated by applicable data processing agreements concluded with the users.

6.2 2. How we use the data

We use your personal data for the following purposes:

6.2.1 2.1 To provide the Services

We may process your personal data to identify you when you login to your account and use our Services, to enable us to operate the Services and provide them to you. This may include verification of your payments, purchase orders and billing information.

6.2.2 2.2 To communicate with you

We may process data of our customers or their individual end-users, in particular email or other contact data, to communicate with our users and end-users, for example, when we assist them with setting up or administering their account, when we provide customer care and support, send technical notices, updates of upcoming changes or improvements to the Services, reminders, security alerts and other support and administrative messages.

6.2.3 2.3 To provide a better user experience

We may process your personal data to learn how you use our Services and thereby continuously enhance user experience as well as provide seamless customer care. We may process such personal data also to improve and enhance our existing Services and develop new offerings. This includes product and market statistics, research and analytics, benchmarks and other analyses to better understand your needs and the needs of users in the aggregate, diagnose problems and analyse trends.

6.2.4 2.4 To protect our Services and defend our or third-party rights

We process your personal data to keep the Service safe, secure and reliable. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm MyQ, our customers and end-users.

We may process some of the data specified in Section 1.1 when required by law or to establish, exercise or defend our legal claims or, where necessary, protect rights and interests of MyQ.

6.2.5 2.5 For marketing and sales purposes

We may process the contact details of the contact persons designated by you or your end-users in order to provide you with information relating to new features of the Services and new product offerings. For more details, please see Section 7 below.

6.3 3. Lawful basis

For the purposes specified in Sections 2.1 and 2.2, we process your personal data based on our contract with you (if you are our direct customer and an individual) or based on our legitimate interest to provide our Services to our customers (where our customer is your company or organisation and you are an authorized end-user designated by your company or organization).

For the purposes specified in Section 2.3, we process your personal data based on our legitimate interest to develop and improve our Services.

For the purposes specified in Section 2.4, we process your personal data based on our legitimate interest to protect and secure our rights or claims or the rights of our customers or users.

For the purpose specified in Section 2.5, we process your personal data based on your voluntary consent where you have given us such consent. In a limited scope permissible under applicable law, we may also use your electronic contact details to inform you about our Services without your explicit consent, based on our legitimate interest, as described in more detail in Section 7 below.

Where we use your personal data for our legitimate interests, we make sure that we take into account any potential impact that such use may have on you. Our legitimate interests don't automatically override yours and we won't use your information if we believe your interests should override ours unless we have other grounds to do so (such as performance of contract, your consent or a legal obligation). If you have any

concerns about our processing, please refer to details of “Your rights” in Section 9 below.

6.4 4. Retention periods

Where we process personal data as data controller, we retain your personal data for the period necessary to fulfil the purposes outlined in this Privacy Policy and/or any Services agreement, unless a longer retention is required by law (e.g. for tax or accounting purposes or due to other legal requirements) or storing of the data is needed for the establishment, exercise or defence of MyQ’s legal claims; in such case, we will store only the data necessary for the enforcement of our claims or our defence for the period necessary in the given case and not exceeding the statutory limitation periods.

Where we process personal data on behalf of our customers as a data processor, we retain such data for the duration of our agreement with such customers and delete them in accordance with our retention and backup processes automatically within 90 days after termination of the agreement, unless the customers ask us to erase them earlier.

6.5 5. Sharing your personal data for legal and business purposes

We may use and/or disclose to third parties (including government bodies and law enforcement authorities, our affiliates, professional advisors and our vendors or subcontractors) information about you when:

- Complying with legal process;
- Enforcing or defending the legal rights of MyQ, and in connection with a corporate restructuring such as a merger, business acquisition or insolvency situations;
- Preventing fraud or imminent harm; and
- Ensuring the security and operability of our network and services.

This information will be shared provided that, in all such circumstances, we will only share the limited personal information that is required to be shared in the unique situation.

We share your data with our trusted business partners or individuals who process your data as our data processors on our behalf and pursuant to our instructions, in accordance with this Privacy Policy. We select our vendors very carefully and always ensure that they provide adequate data protection and security safeguards. To this

effect, we have bound our data processors with data processing agreements concluded pursuant to Article 28 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR").

If you select your Services tenant in the MyQ administration interface to be located in the EU, then your Customer Data will be processed in the EU, in accordance with Microsoft's EU Data Boundary contractual commitments. If you select your Services tenant in the MyQ administration interface to be located outside the EU, such transfer will be made based on Standard Contractual Clauses (model clauses) approved by the European Commission (2010/87/EU), unless a different transfer mechanism under Articles 45, 46 et seq. of the GDPR becomes available. Notwithstanding the above, your Customer Data may also be transferred to countries for which the European Commission has issued an adequacy decision.

The list of our current processors who may have access to your personal data:

- http://salesforce.com EMEA Ltd. (sales-related processed and technical support),
- Microsoft Ireland Operations Limited (collaboration and communication, Microsoft Azure – cloud hosting services),
- TeamViewer GmbH (technical support).

Apart from the processors mentioned above, we may also share your personal data to manage our business processes and comply with our legal obligations, including logistical, invoicing, tax, legal and technical services.

Apart from third-party vendors, MyQ may share data with its affiliates located in the EU and UK for the purpose of certain logistical, invoicing, tax, legal and technical services. The updated list of our EU and UK affiliates is available at https://www.myq-solution.com/en/the-list-of-myq-data-processors .

6.6 6. Anonymous statistics

We may use aggregated anonymized data derived from the personal data provided by you or collected by the program analytics such as user behavior and activities for our own statistics, for auditing, for the purposes of product and market research, for analytics (which helps us to optimize and improve our Services and their usability, the range of Services and to develop new technologies, products, and services), and for benchmarks and other analyses.

6.7 7. Marketing communications

We may contact the contact persons designated by you or your end-users in order to provide information relating to new features of the Services and new product offerings, provided that we have the requisite permission to do so, either on the basis of your consent (where we have requested it and you have provided it to us), or our legitimate interests to provide you with marketing communications where we may lawfully do so, within the limits provided by law. In the latter case, we will only send you marketing communications if you are using or have recently used any of our Services and have not objected to receiving such information (by any means mentioned below).

Your marketing communication preferences may be changed at any time by following the instructions below:

- If you would like to unsubscribe from an email sent to you, follow the 'unsubscribe' link and/or instructions placed at the bottom of the email.
- Alternatively, you can contact us using the details in the "Contact Us" section below to change your marketing communication preferences, including the withdrawal of your consent.

If you have received unwanted, unsolicited emails sent via our system or purporting to be sent via our system, please forward a copy of that email with your comments to info@myq-solution.com[1] for review.

Please note that we may occasionally send you important information (including via email) about our Services that you are using or have used including changes to applicable terms and conditions and/or other communications or notifications as may be required to fulfil our legal and contractual obligations, as described in Section 2.2 above. These important Service communications do not constitute marketing communication are not affected by your preferences.

6.8 8. Security and location of your data

We have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines in accordance with good industry practice while keeping in mind the state of technological development in order to protect your data against accidental loss, destruction, alteration, unauthorized disclosure or access or unlawful destruction. Such measures may include, without limitation, taking reasonable steps to ensure the reliability of

1. mailto:info@myq-solution.com

employees having access to your data and providing for limited access rights and access controls; authentication; personnel training; regular back up; data recovery and incident management procedures; restrictions on storing, printing and disposal of personal data; software protection of devices on which personal data are stored; etc.

6.9 9. Your rights

This Section describes your rights under the applicable laws, such as the GDPR, and how to apply them. If you exercise any of your rights pursuant to this Section or pursuant to applicable laws, we will communicate any rectification or erasure of your personal data or restriction of processing carried out in accordance with your request to each recipient to whom the personal data have been disclosed pursuant to Section 5 of this Privacy Policy, unless such communication proves impossible or involves disproportionate effort.

If you wish to exercise these rights and/or obtain all relevant information about the processing of your personal data, please contact us at info@myq-solution.com[2]. You will be asked to identify yourself; this is necessary to verify that the request has been sent by you. We will respond within 1 month after receipt of your request, but we retain the right to extend this period up to 2 months in exceptional justified circumstances. We will in any event inform you within 1 month after receipt of your request if we decide to extend the period for our response.

In accordance with applicable laws and as further described below, you have the right to request access to your personal data and information about their processing, the right to rectification, erasure or portability (e.g., transfer of your personal data to another service provider) of your personal data we process, as well as the right to object to the processing of your personal data and/or request restriction of such processing.

Please note that your objection to processing could mean that we are unable to provide you with our Services or otherwise perform the actions necessary to achieve the purposes set out above (see Section 2 ‘How we use the data’).

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us by contacting us via the contact details in Section 10 ‘Contact Us’.

2. mailto:info@myq-solution.com

6.9.1 9.1 Information about, access to and rectification of your personal data

According to applicable laws, you have the right to obtain confirmation as to whether or not personal data concerning you are being processed (pursuant to the process described above), and, where that is the case, the right to access and rectify your personal data you have shared with us. Through your settings of the Services, you can access and update your account information and change your profile settings.

6.9.2 9.2 Accuracy of your personal data

We take reasonable measures to ensure that you are able to keep your personal data accurate and updated. You can always approach us in order to obtain confirmation whether or not we still process your personal data.

If you find out that your personal data processed by us is inaccurate or incomplete and you are unable to update your personal data according to Section 9.1 of this Privacy Policy, you may request us to update such personal data. We will verify your identity and update your personal data on your behalf.

6.9.3 9.3 Erasure of your personal data

You can ask us to erase your personal data at any time. If you approach us with such a request, we will delete all your personal data we have without undue delay, provided that your personal data is no longer necessary for the provision of the Services or other permitted purposes, in particular in connection with exercising and defending our legal rights, or meeting our legal obligations. We will also delete (and ensure deletion by the processors that we engage) all your personal data in case you withdraw your consent or in the circumstances that the law requires us to do so.

6.9.4 9.4 Restriction of processing

If you request us to restrict the processing of your personal data, e.g. in circumstances when you contest the accuracy, lawfulness or our need to process your personal data, we will limit processing of your personal data to the necessary minimum (storage) and, if applicable, will process them only for the establishment, exercise or defence of legal claims or, where necessary, for protection of rights of another natural or legal person, or other limited reasons dictated by the applicable law. In case the restriction is lifted, and we continue processing your personal data, you will be informed accordingly without undue delay.

6.9.5 9.5 Portability of your personal data

You have the right to receive personal data relating to you and which you have provided to us. If you approach us with such request, we will provide your personal data in commonly used and machine-readable format to you without undue delay from receipt of your request. If you request so, we will send your personal data to a third party (another data controller) which you will identify in your request, unless such request would adversely affect rights or freedoms of others and where technically feasible.

6.9.6 9.6 Objection to processing

You have the right to object to our using your personal data on the basis of our legitimate interests. In such case, we will no longer process your personal data unless we demonstrate compelling legitimate grounds for their further processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of our legal claims. If you object to processing of your data for direct marketing purposes, we will cease to process your data for these purposes.

6.9.7 9.7 Withdraw your consent

If you have provided us any consent with the processing of personal data, for example for marketing communication, you can withdraw your given consent at any time without stating any reason. We will block your personal data for any further processing. Please note that the withdrawal of your consent does not affect the lawfulness of any processing based on consent before its withdrawal.

6.9.8 9.8 Complaint to a data protection authority

You have the right to submit a complaint concerning our data processing activities to Úřad pro ochranu osobních údajů, at Pplk. Sochora 2Z, 170 00 Praha 7, Czech Republic.

6.9.9 9.9 Request to opt out of the sale of personal data under the CCPA

MyQ does not sell, as defined in the CCPA, any personal data. Therefore, if a California consumer communicates an opt-out request under this provision, it will have no effect. If you require additional information about your rights under the CCPA to opt out of the sale of your personal data, please contact: info@myq-solution.com[3].

6.10 10. Contact Us

If you have any queries regarding our data collection and protection practices or your rights, please do not hesitate to contact us at info@myq-solution.com[4].

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

7 Server Uptime, Data Backup, and Disaster Recovery

7.1 Server Uptime

MyQ Roger is dedicated to maintaining a 99.9% uptime target; however, service level agreements (SLAs) are tailored per customer and do not explicitly guarantee this metric. We employ advanced high-availability (HA) strategies, leveraging multi-zone deployments and multi-pod architectures to ensure service continuity and minimize potential downtime in the event of operational disruptions.

7.2 Real-Time System Status Monitoring

To enhance transparency and provide real-time visibility into system performance, we maintain a dedicated status site that delivers up-to-date insights on service health. This platform enables customers to:

- **Monitor Live System Status**: View real-time operational metrics and incident updates.
- **Receive Proactive Notifications**: Subscribe to alerts for service degradation or planned maintenance events.
- **Access Historical Uptime Reports**: Review past incidents and performance trends to assess reliability.

By offering a centralized status site, we empower customers with timely and accurate information, reinforcing trust and enabling proactive decision-making in the event of disruptions.

7.3 Backup Strategies

7.3.1 Azure SQL Backup Strategy

We employ a geo-redundant backup strategy for Azure SQL databases, ensuring data resilience and recoverability. Key aspects include:

- **Geo-Redundant Storage**: Backups are replicated across multiple regions for disaster recovery.
- **Retention Policy**: Backups are retained for several months, allowing historical data recovery.
- **Incremental Backups**: A 14-day point-in-time recovery (PITR) window enables granular restoration of lost data.

- **SLA-Based Customization**: Retention periods and recovery time objectives (RTO) vary based on cluster-specific SLAs and can be tailored to meet customer needs.

7.3.2 Azure Cosmos DB Backup Strategy

For Azure Cosmos DB, we implement comprehensive data protection mechanisms, particularly for accounting records, ensuring data integrity and traceability:

- **Full Accounting Data Reports**: All accounting transactions, including job accounting for print, scan, copy, and fax activities, are fully recorded.
- **Historical Data Retracing**: Our system allows tracking and retracing of any reported accounting records to ensure compliance and auditability.
- **High Availability and Redundancy**: Built-in multi-region replication ensures continuity and minimizes data loss risks.

By implementing these robust backup strategies, we safeguard critical business data while providing flexible recovery options tailored to customer-specific SLAs.

7.4 Disaster Scenarios & Response Plan

Disaster Scenario	Mitigation Strategy	Recovery Process
Data Corruption	PITR (Point-in-Time Recovery)	Restore database to last known good state
Cloud Region Outage	Geo-redundant backups & failover	Switch to secondary Azure region
Kubernetes Node Failure	Auto-replication of services in AKS	Pods are rescheduled to healthy nodes
Cyberattack (DDoS, Ransomware, etc.)	WAF, Azure DDoS Protection, and security monitoring	Isolate compromised systems, restore from clean backups

8 Zero Trust

8.1 Understanding Zero Trust Security

Trust is a complex construct. For example, I trust my mother to cook a perfect dinner, but I would never trust her with network security. In cybersecurity, misplaced trust can lead to significant vulnerabilities, which is why the Zero Trust model exists.

8.1.1 Real-World Example: The Danger of Implicit Trust

One of the most well-known breaches where a lack of Zero Trust principles played a role was the **Colonial Pipeline attack** in 2021. Attackers gained access through a compromised VPN credential, which did not have Multi-Factor Authentication (MFA) enabled. Since the network implicitly trusted authenticated users, the attackers were able to move laterally and deploy ransomware, causing widespread fuel shortages across the U.S. This incident highlights why "never trust, always verify" is critical to modern cybersecurity.

8.2 What is Zero Trust?

Zero Trust is a cybersecurity paradigm built on the principle of "never trust, always verify." It ensures that users and devices are not trusted by default, even if they are connected to a secured corporate network or were previously verified. Instead, trust must be continually assessed and validated based on various security signals.

8.2.1 The Core Principles of Zero Trust

Zero Trust is defined in **NIST SP 800-207** as a framework focused on resource protection through continuous verification. This security model applies to:

- **Identity and Access Management**: Ensuring users and devices authenticate securely.
- **Network and Endpoint Security**: Protecting communication and enforcing strict access controls.
- **Data Protection**: Ensuring sensitive data is encrypted and securely stored.
- **Continuous Monitoring**: Detecting anomalies and responding to potential threats in real time.

8.3 How Zero Trust Applies to MyQ Roger

8.3.1 Explicit Verification

- Authentication is required even on authorized devices (phones/desktops).
- Uses modern authentication standards.
- Multi-Factor Authentication (MFA) is enforced for mobile and Multi-Function Printer (MFP) logins.
- OAuth2 Device Flow is implemented for device authorization.
- **Continuous authentication mechanisms** track changes in user behavior to detect anomalies.

8.3.2 Access Management

- **Role-Based Access Control (RBAC)** ensures users have only the minimum necessary access.
- **Least Privilege Principle** is enforced to reduce security risks.
- **Micro-Segmentation** is implemented to limit lateral movement within the network.
- **Just-in-Time (JIT) Access Controls** dynamically adjust user privileges based on the context.

8.3.3 Device & Endpoint Security

- Unique access tokens are issued for each device type.
- Transport Layer Security (TLS) is mandatory for all communications.
- **Endpoint Detection and Response (EDR) solutions** monitor and analyze device behavior.
- **Zero Trust Network Access (ZTNA)** ensures that only authorized devices can access specific resources.

8.3.4 Data Protection

- All data is securely stored using encrypted storage solutions.
- Policies ensure data is accessed only by authorized entities.
- **Data Loss Prevention (DLP) solutions** monitor and prevent unauthorized data exfiltration.
- **Secure Enclaves** protect highly sensitive data from unauthorized access.

8.4 Addressing Cyber Threats with Zero Trust

Zero Trust helps mitigate the following threats:

- **Insider threats**: Prevents employees or compromised accounts from gaining unauthorized access.

- **Credential stuffing and phishing attacks**: Reduces the impact of compromised credentials through continuous authentication.
- **Lateral movement attacks**: Micro-segmentation restricts attackers from moving laterally across networks.
- **Supply chain attacks**: Ensures strict verification of third-party access and integrations.

8.5 Compliance and Regulatory Considerations

Zero Trust aligns with various cybersecurity regulations and frameworks:

- **ISO 27001**: Enforces secure access management and data protection.
- **GDPR**: Ensures secure processing and storage of personal data.
- **HIPAA**: Protects sensitive healthcare information.
- **NIST Cybersecurity Framework**: Provides guidelines for Zero Trust implementation.

8.6 Why Zero Trust Matters

Adopting Zero Trust minimizes the risk of security breaches, insider threats, and unauthorized access. In an era of increasing cyber threats, a Zero Trust architecture provides robust protection by ensuring continuous verification and strict access controls across all resources.

By implementing these principles, MyQ Roger ensures a secure, resilient, and adaptive security posture that aligns with modern cybersecurity best practices. Additionally, continuous monitoring, access controls, and real-time threat detection enhance the organization's ability to respond to evolving cyber threats effectively.

9 Secure Login with MyQ Roger

9.1 Introduction

Using a PIN as the primary method of login was never truly secure. Early mobile phones relied on PINs, but as security concerns evolved, so did authentication methods. Today, biometrics have become the norm, offering a more secure and user-friendly approach to authentication.

MyQ Roger embraces this shift by implementing the latest OAuth 2.0 Device Authorization Grant (formerly known as the Device Flow). This modern authentication method requires users to log in using a one-time QR code scanned with their mobile phone, eliminating the need for static passwords or insecure PINs.

We recognize a user's mobile phone as one of the most secure means of authentication. By leveraging biometric authentication to unlock the phone and subsequently access the MyQ app, we ensure that the individual logging in is the legitimate owner of the account.

9.2 Secure Authentication with MyQ Roger

- **OAuth 2.0 Device Authorization Grant**: Instead of relying on traditional PINs, users authenticate using a dynamically generated QR code. This method significantly reduces the risk of credential theft or reuse attacks.
- **Biometric Verification**: Since modern smartphones require biometric verification (e.g., fingerprint or facial recognition) to unlock, this adds an extra layer of security before accessing MyQ Roger.

9.3 Legacy PIN Authentication

While MyQ Roger still provides PIN-based login as an option, it is considered an insecure method and is discouraged by default. Users who choose to enable PIN authentication must explicitly mark it as safe, acknowledging the associated security risks. Furthermore, enabling PIN login will disable some advanced security features to mitigate potential vulnerabilities.

9.4 Security Responsibility

If an organization opts to allow PIN-based login, the responsibility for maintaining a secure environment falls on the customer. Best practices such as enforcing strong PIN policies, implementing physical security measures, and monitoring access logs should be followed to minimize risks.

9.5 Conclusion

With MyQ Roger, we prioritize security by leveraging modern authentication standards. The adoption of mobile-based biometric authentication ensures a seamless yet secure user experience. While legacy PIN-based login remains available, it is not the recommended method, and customers must take additional precautions if they choose to use it. By embracing secure login mechanisms, organizations can enhance both security and usability for their users.

10 Secure Printing with MyQ Roger

10.1 The Challenge of Secure Printing

Traditional secure printing methods rely on physically tethered connections, such as LPT cables, where a dedicated printer is assigned to a single laptop. While this method ensures the highest level of security, it is impractical in modern environments that demand flexibility, mobility, and shared resources.

AirPrint and Mopria offer secure printing capabilities but are insufficient in scenarios where users can initiate remote print jobs without being physically present near the printer. This creates security vulnerabilities where sensitive documents might be left unattended.

10.2 MyQ Roger: A Comprehensive Secure Printing Solution

MyQ Roger integrates multiple printing workflows while enforcing security protocols to ensure that users must be physically present to authenticate and release print jobs. The system guarantees that print jobs are securely stored and transmitted while minimizing data exposure.

10.3 Secure Printing Methods in MyQ Roger

10.3.1 Direct PC-to-Printer Printing

- Utilizes **IPP/s (Internet Printing Protocol Secure)** to transfer print jobs securely.
- Supported printer brands: **Ricoh, Kyocera**.
- Print jobs remain stored directly on the printer until the user authenticates and releases the job.

10.3.2 MyQ Roger Client (MRC)

- Print jobs are **encrypted and stored locally** on the user's PC.
- The printer retrieves the encrypted file **only after user authentication**.
- Secure printing is executed via **IPP/s**.

10.3.3 Cloud Printing

- Print files are securely stored in the user's cloud storage (e.g., **OneDrive, Google Drive, Dropbox**).
- The printer downloads the document directly from cloud storage using a **short-lived access link**.

- **No document retention** on the printer after printing, ensuring data confidentiality.

10.3.4 Microsoft Universal Print Integration

- MyQ Roger implements a **Universal Print Connector** that enables printers to communicate directly with **Microsoft's Universal Print servers**.
- Print jobs are securely stored on **Microsoft servers** and retrieved on demand after user authentication.
- Printing is conducted through **Universal Print drivers**, ensuring seamless and secure job handling.

10.4 Conclusion

MyQ Roger delivers a **holistic, secure printing environment** by combining direct, local, and cloud-based printing workflows with robust security measures. By requiring users to authenticate in person before job execution, MyQ Roger eliminates the risks associated with unattended print jobs, ensuring maximum data protection in modern workplaces.

11 Business Contacts

MyQ® Manufacturer	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prague 9, Czech Republic ID no. 615 06 133 MyQ® spol. s r.o. is registered in the Commercial Register at the Municipal Court in Prague, file no. C 29842 (hereinafter as "MyQ®")
Business information	http://www.myq-solution.com info@myq-solution.com[5]
Technical support	support@myq-solution.com[6]
Notice	MANUFACTURER WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY INSTALLATION OR OPERATION OF THE SOFTWARE AND HARDWARE PARTS OF THE MyQ® PRINTING SOLUTION. This manual, its content, design and structure are protected by copyright. Copying or other reproduction of all or part of this guide, or any copyrightable subject matter without the prior written consent of MyQ® is prohibited and can be punishable. MyQ® is not responsible for the content of this manual, particularly regarding its integrity, currency and commercial occupancy. All the material published here is exclusively of informative character. This manual is subject to change without notification. MyQ® is not obliged to make these changes periodically nor announce them, and is not responsible for currently published information to be compatible with the latest version of the MyQ® printing solution.

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

Trademarks	“MyQ®”, including its logos, is a registered trademark of MyQ®. Any use of trademarks of MyQ® including its logos without the prior written consent of MyQ® Company is prohibited. The trademark and product name are protected by MyQ® and/or its local affiliates.

myQ roger

SAVE TIME WITH PERSONALIZED PRINT SOLUTIONS

MyQ Roger is a cloud native solution built for modern cloud-first offices, simplifying document workflows, enabling secure browsing, printing, and scanning wherever users are.

info@myq-solution.com

myq-solution.com

50+ million
Trusted users

1+ million
Active devices

26+
Brands supported

1000+
Certified partners

Operating in **140+** countries

Awarded and certified

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001