MyQ Roger Datensicherheit Whitepaper 2.x

DEUTSCH

Generiert aus docs.myq-solution.com
August/2026
Copyright © 2026 MyQ spol. s r.o. Alle Rechte vorbehalten.

Hinweis zur Übersetzung

Diese Übersetzung wurde mithilfe künstlicher Intelligenz erstellt. Bei Abweichungen oder Unklarheiten ist das englischsprachige Quelldokument maßgeblich.

Inhaltsverzeichnis

1 Einleitung ... 5
2 Glossar ... 6
3 Betriebssicherheit ... 7
3.1 Einleitung ... 7
3.2 Überwachung ... 7
3.3 Verwaltung von Schwachstellen ... 9
3.4 Infrastruktursicherheit ... 9
3.5 Entwicklungs-Workflow ... 10
3.6 Fazit ... 11
4 Anwendungssicherheit ... 12
4.1 Die Entwicklung von Sicherheitsbedrohungen ... 12
4.2 Der Sicherheitsansatz von MyQ Roger ... 12
4.3 Shifting Left in der Sicherheit ... 13
4.4 Sicherheitsverantwortlichkeiten von MyQ ... 13
4.5 MyQ Roger Sicherheitskontrolle/-management ... 13
4.6 Microsoft Azure und Compliance ... 14
4.7 Sicherheitsverantwortlichkeiten der Kunden ... 15
4.8 Sicherheitsautomatisierung ... 15
4.9 Fazit ... 16
5 Datenschutz ... 17
5.1 Übersicht ... 17
5.2 Multi-Tenant-Cloud-Sicherheit ... 17
5.3 Verschlüsselung und sichere Kommunikation ... 17
5.4 Compliance und Identitätsmanagement ... 18
5.5 DSGVO-Konformität ... 18
5.6 Datensicherungen ... 19
6 Datenschutzrichtlinie ... 20
6.1 1. Daten, die wir erfassen oder erhalten ... 20
6.2 2. Wie wir die Daten verwenden ... 22
6.3 3. Rechtsgrundlage ... 23
6.4 4. Aufbewahrungsfristen ... 24
6.5 5. Weitergabe Ihrer personenbezogenen Daten für rechtliche und geschäftliche Zwecke ... 25

6.6 6. Anonyme Statistiken ... 26
6.7 7. Marketingmitteilungen ... 27
6.8 8. Sicherheit und Speicherort Ihrer Daten ... 27
6.9 9. Ihre Rechte ... 28
6.10 10. Kontakt ... 32
7 Server-Betriebszeit, Datensicherung und Disaster Recovery ... 33
7.1 Server-Verfügbarkeit ... 33
7.2 Echtzeit-Überwachung des Systemstatus ... 33
7.3 Sicherungsstrategien ... 33
7.4 Katastrophenszenarien und Notfallplan ... 34
8 Null Vertrauen ... 36
8.1 Zero-Trust-Sicherheit verstehen ... 36
8.2 Was ist Zero Trust? ... 36
8.3 Wie Zero Trust auf MyQ Roger angewendet wird ... 37
8.4 Bekämpfung von Cyber-Bedrohungen mit Zero Trust ... 38
8.5 Compliance- und regulatorische Überlegungen ... 38
8.6 Warum Zero Trust wichtig ist ... 38
9 Sicheres Login mit MyQ Roger ... 39
9.1 Einleitung ... 39
9.2 Sichere Authentifizierung mit MyQ Roger ... 39
9.3 Legacy-PIN-Authentifizierung ... 39
9.4 Verantwortung für die Sicherheit ... 40
9.5 Fazit ... 40
10 Sicheres Drucken mit MyQ Roger ... 41
10.1 Die Herausforderung des sicheren Druckens ... 41
10.2 MyQ Roger: Eine umfassende Lösung für sicheres Drucken ... 41
10.3 Sichere Druckmethoden in MyQ Roger ... 41
10.4 Fazit ... 42
11 Geschäftskontakte ... 43

1 Einleitung

Der Zweck dieses Dokuments besteht darin, die Kunden von MyQ Roger über Prozesse zu informieren, die die Herstellung von Verbindungen im System betreffen, sowie über Sicherheitsmaßnahmen, die zum Schutz der daraus resultierenden Datenübertragung getroffen werden.

2 Glossar

- **IPP/s (Internet Printing Protocol über Secure TLS)**:
  - MyQ Roger gewährleistet sicheres Drucken durch die Verwendung des Internet Printing Protocol (IPP) über einen TLS-verschlüsselten Kanal, wodurch unbefugter Zugriff verhindert und die Datenintegrität während der Übertragung gewährleistet wird.
  - MyQ Roger optimiert den Netzwerkverkehr durch effiziente Paketverarbeitung, reduziert unnötige Datenübertragungen und gewährleistet eine sichere Kommunikation zwischen den Endpunkten.
- **TLS (Transport Layer Security)**:
  MyQ Roger erzwingt TLS 1.2/1.3 für eine sichere Datenverschlüsselung bei allen Kommunikationen und gewährleistet so Schutz vor Abhör- und Man-in-the-Middle-Angriffen (MITM).
- **Speicherte Daten, Daten während der Übertragung**:
  - **Speicherte Daten**: MyQ Roger verschlüsselt gespeicherte Daten mit AES-256 und gewährleistet so, dass sensible Informationen vor unbefugtem Zugriff geschützt sind.
  - **Daten während der Übertragung**: Alle zwischen Clients, Servern und Cloud-Diensten übertragenen Daten werden mit TLS verschlüsselt, um Integrität und Vertraulichkeit zu gewährleisten.
- **Zero-Trust-Infrastruktur**:
  MyQ Roger folgt einem **Zero-Trust**-Sicherheitsmodell, indem es eine kontinuierliche Authentifizierung, Geräteüberprüfung und Zugriff mit geringsten Privilegien für Benutzer und Dienste implementiert.
- **IAM (Identity and Access Management)**:
  MyQ Roger integriert IAM-Best Practices, indem es eine sichere Benutzerauthentifizierung, Multi-Faktor-Authentifizierung (MFA) und identitätsbasierte Zugriffskontrollen durchsetzt.
- **RBAC (rollenbasierte Zugriffskontrolle)**:
  MyQ Roger implementiert RBAC, um Berechtigungen basierend auf Benutzerrollen einzuschränken und sicherzustellen, dass nur autorisiertes Personal auf kritische Funktionen und sensible Daten zugreifen kann.
- **SSO (Single Sign-On)**:
  MyQ Roger unterstützt **SSO** über die OAuth2-Integration und ermöglicht so eine nahtlose Authentifizierung über Unternehmensanwendungen hinweg unter Wahrung der Sicherheit und Compliance.

3 Betriebssicherheit

3.1 Einleitung

Sicherheit hat bei MyQ Roger oberste Priorität. Wir verfolgen einen Sicherheitsansatz in jeder Phase der Entwicklung, Bereitstellung und des Betriebs. Angesichts der kritischen Natur von Cloud-Umgebungen muss die Sicherheit **proaktiv, automatisiert und kontinuierlich überwacht** werden, um Verstöße und unbefugten Zugriff zu verhindern.

Unsere **Strategie für sicheren Betrieb** umfasst **kontinuierliche Überwachung, Schwachstellenmanagement, Infrastruktursicherheit und Compliance,** um die Integrität von Anwendungen und Infrastruktur zu gewährleisten.

3.2 Überwachung

Eine kontinuierliche Überwachung ist unerlässlich, um Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren. MyQ verfolgt einen **mehrschichtigen Überwachungsansatz:**

3.2.1 Endpoint Detection and Response (EDR)

- Überwacht alle Endpunkte (Server, VMs und Container) auf verdächtige Aktivitäten.
- Verwendet **Verhaltensanalysen und Bedrohungsinformationen,** um fortgeschrittene Bedrohungen zu erkennen.
- Isoliert automatisch kompromittierte Endpunkte, um eine laterale Ausbreitung zu verhindern.

3.2.2 Azure Defender (jetzt Defender for Cloud)

- Schützt **Azure AKS, SQL Server, virtuelle Maschinen und Speicher**.
- Bietet **Echtzeit-Bedrohungserkennung** und Empfehlungen zur Sicherheitskonfiguration.
- Integriert sich in **Microsoft Sentinel (SIEM)** für zentralisierte Warnmeldungen.

3.2.3 Host-Scan

- Scans **VMs, Cloud-Instanzen und lokale Server** auf Fehlkonfigurationen und veraltete Software.
- Erkennt **Risiken durch Privilegieneskalation, unbefugte Zugriffspunkte und veraltete Abhängigkeiten**.

3.2.4 Protokollsammlung und -analyse

- **Zentralisierte Protokollierung** auf einem separaten Cluster für Skalierbarkeit und Isolierung.
- **Protokolle aus Kubernetes, Anwendungen und Infrastruktur** werden für eine effiziente Abfrage gekennzeichnet**.**
- **Langfristige Aufbewahrungsrichtlinien** gewährleisten Compliance und Sicherheitsanalysen.
- **Warnmechanismen** erkennen Anomalien und Sicherheitsvorfälle und lassen sich in SIEM integrieren.
- **Echtzeit-Protokollkorrelation** für API-Anfragen, Authentifizierungsereignisse, Datenbankabfragen und Firewall-Datenverkehr.

3.2.5 Port-Scanning

- Erkennt unbefugte **offene Ports**, die Dienste Gefahren aussetzen.
- Verwendet **automatisierte Tools wie Nmap und ZMap,** um nach **unerwarteten Portänderungen** zu suchen.

3.2.6 Container-Scanning

- **Statisches und dynamisches Scannen** von Docker-Containern vor der Bereitstellung.
- Identifiziert Schwachstellen in **Basis-Images, Anwendungsschichten und Laufzeitberechtigungen**.
- Integriert mit **Trivy** für **das Scannen von Images auf Sicherheitslücken**.

3.2.7 Kubernetes-Überwachung

- Verwendet **die in Azure Kubernetes Service (AKS) integrierte Überwachung** mit **Prometheus und Grafana**.
- Überwacht **Kubernetes-API-Aufrufe, RBAC-Richtlinien und Pod-Sicherheit**.
- Warnungen bei **Container-Privilegienerweiterungen, übermäßiger Ressourcennutzung und Versuchen lateraler Bewegungen**.

3.2.8 Regelmäßige TLS-Scans

- MyQ führt **TLS-Sicherheitsscans mit Qualys SSL Labs** durch, um Best Practices sicherzustellen.
- TLS-Konfigurationen werden bewertet, um eine **A+ Sicherheitsbewertung** aufrechtzuerhalten und Risiken durch schwache Protokolle zu minimieren.
- Automatisierte Tools überprüfen **die Gültigkeit von Zertifikaten, verfolgen deren Ablauf und überprüfen die Protokollstärke**.

3.3 Verwaltung von Schwachstellen

3.3.1 Schwachstellenscans

- **Regelmäßige Scans** erkennen Sicherheitslücken in Anwendungen und Infrastruktur.
- Beinhaltet **automatisierte CVE-Scans** für in der Cloud bereitgestellte Komponenten.
- Integriert mit **DefectDojo, SonarQube und Trivy** für die Risikobewertung.

3.3.2 Penetrationstests

- Werden regelmäßig durchgeführt, um Sicherheitslücken zu identifizieren, bevor sie ausgenutzt werden können.
- Kombiniert **automatisierte und manuelle Testmethoden** für eine umfassende Bewertung.
- Die Ergebnisse werden **dokumentiert, priorisiert und** entsprechend **behoben**.

3.4 Infrastruktursicherheit

Eine **gehärtete Infrastruktur** gewährleistet Sicherheit, die über die reine Überwachung hinausgeht. MyQ setzt Folgendes ein:

3.4.1 SIEM (Security Information and Event Management)

- **Microsoft Sentinel SIEM** sammelt Sicherheitsereignisse für die Echtzeit-Erkennung.
- Analysiert Protokolle von **Firewalls, Identitätssystemen, Anwendungsprotokollen, Audit-Protokollen und Bedrohungs-Feeds**.
- Ermöglicht **automatisierte Reaktionen auf erkannte Bedrohungen**.

3.4.2 Sicherheitsüberwachung und -management

- **Die Jira-Fehlerdatenbank** verfolgt, kategorisiert und priorisiert Sicherheitslücken.
- **DefectDojo** konsolidiert Testergebnisse und gewährleistet so eine strukturierte Nachverfolgung von Sicherheitsmaßnahmen.
- Regelmäßige **Patches und Korrekturen** sorgen für eine hohe Sicherheit.

3.4.3 Identitäts- und Zugriffsmanagement (IAM)

- Setzt **Zero Trust** mit **rollenbasierter Zugriffskontrolle (RBAC) und Multi-Faktor-Authentifizierung (MFA)** durch.
- Verwendet **Azure AD** für die Identitätsverwaltung.

- **Warnmeldungen bei Privilegienerweiterungen** erkennen unbefugten Administratorzugriff.

3.5 Entwicklungs-Workflow

Die sichere Softwareentwicklung ist ein wichtiger Aspekt der Sicherheitsstrategie von MyQ. Die folgenden Maßnahmen gewährleisten die Integrität von Code, Pipelines und Cloud-Umgebungen:

3.5.1 Sichere Entwicklungsumgebung

- Die Entwickler von MyQ verwenden **sicherheitsgehärtete Umgebungen** mit Endpunktschutz.
- Entwickler müssen **sichere Codierungspraktiken** befolgen **und regelmäßig an Sicherheitsschulungen** teilnehmen.

3.5.2 GitLab Secure Pipelines

- GitLab CI/CD-Pipelines umfassen **automatisierte Sicherheitsüberprüfungen, Code-Reviews und Tests**.
- **Statische Anwendungssicherheitstests (SAST)** und **dynamische Anwendungssicherheitstests (DAST)** erkennen Schwachstellen.
- **Container Image Signing** stellt sicher, dass nur vertrauenswürdige Images bereitgestellt werden.

3.5.3 IAM und Zugriffskontrolle

- Nur **ausgewählte DevOps- und SecOps-Mitarbeiter** haben Zugriff auf Azure-Cloud-Umgebungen.
- Es wird **eine rollenbasierte Zugriffskontrolle (RBAC) mit Just-In-Time (JIT)-Privilegienerweiterung auf Mindestniveau** durchgesetzt.

3.5.4 Azure Kubernetes & Containersicherheit

- **Die AKS-Cluster** von MyQ **beziehen Images ausschließlich aus der Azure Container Registry (ACR)**.
- AKS-Umgebungen setzen **Netzwerkrichtlinien und Pod Security Standards (PSS)** durch, um Workloads zu isolieren.

3.5.5 Verwaltung geheimer Daten

- **Alle Geheimnisse und API-Schlüssel werden in Azure Key Vault gespeichert** und sind nur für IAM-autorisiertes Personal zugänglich.
- Vor dem Commit in Git werden **Trivy-Dateisystem-Scans** durchgeführt, um sensible Geheimnisse zu erkennen und zu verhindern.

3.6 Fazit

Die Strategie für sicheren Betrieb von MyQ basiert auf **kontinuierlicher Überwachung, proaktivem Bedrohungsmanagement und starker Infrastruktursicherheit**. Durch den Einsatz **fortschrittlicher Sicherheitstools, strenger Zugriffskontrollen und automatisierter Tests** gewährleistet MyQ eine **sichere und widerstandsfähige Cloud-Umgebung**.

Durch die **Integration von TLS-Sicherheitsscans, Penetrationstests und zentraler Protokollierung** verbessert MyQ seine Fähigkeit, **Sicherheitsrisiken** effektiv zu **erkennen, darauf zu reagieren und sie zu mindern**.

Sicherheit ist eine **sich ständig weiterentwickelnde Herausforderung**, und MyQ ist weiterhin bestrebt, **die Sicherheitsmaßnahmen durch regelmäßige Updates, Compliance-Audits und bewährte Sicherheitsverfahren** zu **verbessern**. Durch die Beibehaltung einer **sicherheitsorientierten Denkweise** gewährleistet MyQ die **Integrität und Vertraulichkeit** seiner Dienste und sorgt so für **Vertrauen und Zuverlässigkeit** für alle Beteiligten.

4 Anwendungssicherheit

4.1 Die Entwicklung von Sicherheitsbedrohungen

In den Anfängen, bevor das Internet weit verbreitet war, wurden Drucker direkt über LPT-Kabel angeschlossen, und die Sicherheitsbedenken waren minimal. Das größte Risiko war physischer Natur – jemand, der einem Benutzer über die Schulter schaute, um gedruckte Dokumente zu sehen. Die Sicherheitslage war überschaubar, und Cyber-Bedrohungen gab es praktisch nicht.

Mit der Vernetzung von Druckern und Geräten hat sich die Bedrohungslage jedoch drastisch verändert. Da Drucker nun über lokale Netzwerke (LANs) und sogar über das Internet zugänglich sind, benötigen Angreifer keinen physischen Zugriff mehr. Bedrohungen wie Man-in-the-Middle-Angriffe (MITM), unbefugtes Abfangen von Daten und Remote-Exploits sind mittlerweile weit verbreitet. Cyberkriminelle haben sich vom Über-die-Schulter-Schauen zum Abhören des Netzwerkverkehrs und Ausnutzen von Schwachstellen weiterentwickelt.

Die Minderung dieser Risiken ist eine ständige Herausforderung, da häufig neue Bedrohungen auftreten. Um diesen sich ständig weiterentwickelnden Sicherheitsherausforderungen zu begegnen, setzt MyQ Roger auf kontinuierliche Sicherheitsmaßnahmen, proaktive Überwachung und starke Abwehrmechanismen.

4.2 Der Sicherheitsansatz von MyQ Roger

MyQ Roger wurde mit einem sicherheitsorientierten Ansatz entwickelt, der sicherstellt, dass Innovation und Benutzererfahrung stets den höchsten Sicherheitsstandards entsprechen. Unser Engagement für Sicherheit spiegelt sich in unseren kontinuierlichen Bemühungen wider, robuste Sicherheitsmaßnahmen in jeder Phase der Entwicklung zu integrieren. Wir verfolgen eine „Secure-by-Default"-Philosophie und integrieren Sicherheit von Grund auf in unsere Produkte und Dienste.

Um dies zu erreichen, nutzt MyQ Roger Automatisierung, datengestützte Risikobewertungen und erstklassige Sicherheitsmaßnahmen, um Bedrohungen proaktiv zu identifizieren und zu mindern. Durch die frühzeitige Implementierung von Sicherheitskontrollen im Entwicklungszyklus nach einem **„Shift-Left"-Ansatz** stellen wir sicher, dass Schwachstellen erkannt und behoben werden, bevor sie in die Produktion gelangen. Diese proaktive Integration ermöglicht es uns, effizient zu skalieren, Risiken zu reduzieren und Sicherheitsbedrohungen zu minimieren. Unser

Ansatz unterstreicht unser Engagement für den Schutz von Kundendaten, Arbeitsabläufen und der allgemeinen Sicherheitslage.

4.3 Shifting Left in der Sicherheit

Shifting Left in der Sicherheit bedeutet, Sicherheit frühzeitig in den Softwareentwicklungslebenszyklus (SDLC) zu integrieren, anstatt Schwachstellen erst später zu beheben. Indem wir Sicherheitsprobleme bereits in den ersten Entwicklungsphasen erkennen, vermeiden wir kostspielige Korrekturen und mindern potenzielle Sicherheitsverletzungen. Diese proaktive Strategie stellt sicher, dass jede Zeile Code den höchsten Sicherheitsstandards entspricht, bevor sie in die Produktion gelangt, wodurch Risiken reduziert und unsere allgemeine Sicherheitslage gestärkt werden.

4.4 Sicherheitsverantwortlichkeiten von MyQ

MyQ Roger hat sich dem Schutz von Kundendaten und der Gewährleistung einer sicheren Betriebsumgebung verschrieben. Zu unseren wichtigsten Sicherheitsverantwortlichkeiten gehören:

- **Datenschutz**: MyQ sorgt dafür, dass Kundendaten sicher gespeichert und verschlüsselt werden, um unbefugten Zugriff zu verhindern und die Vertraulichkeit der Daten zu gewährleisten.
- **Regelmäßige Sicherheitspatches**: Wir wenden proaktiv Sicherheitspatches und Updates auf alle Systeme an, um Schwachstellen zu beseitigen, bevor sie ausgenutzt werden können.
- **Zugriffskontrollmanagement**: Wir setzen strenge Zugriffsrichtlinien nach dem Prinzip der geringsten Privilegien durch und stellen so sicher, dass nur autorisiertes Personal auf sensible Ressourcen zugreifen kann.

Durch die Einhaltung dieser Sicherheitsgrundsätze fördert MyQ Roger eine Sicherheitskultur, die Benutzer vor potenziellen Bedrohungen schützt und gleichzeitig die Einhaltung von Industriestandards gewährleistet.

4.5 MyQ Roger Sicherheitskontrolle/-management

Obwohl wir uns auf eine sichere Cloud-Infrastruktur verlassen, übernimmt MyQ Roger die direkte Verantwortung für die Implementierung zusätzlicher Sicherheitsebenen und die Einhaltung der besten Praktiken der Branche. Unser Ansatz umfasst:

- **Schlüsselverwaltung mit Azure Key Vault**: Wir verwenden Azure Key Vault, um alle Geheimnisse, privaten Schlüssel und Zertifikate sicher zu speichern und

zu verwalten und gewährleisten so strenge Zugriffskontrollen und Verschlüsselung.
- **ISO 27001-Zertifizierung**: Wir halten uns an die ISO 27001-Standards, um einen strukturierten und konsistenten Ansatz für die Informationssicherheit zu gewährleisten.
- **Endpoint Detection and Response (EDR)**: Wir nutzen fortschrittliche EDR-Lösungen, um Sicherheitsbedrohungen in Echtzeit zu erkennen, zu analysieren und zu mindern, wodurch die Reaktionszeit verkürzt und Risiken minimiert werden.
- **Sichere Entwicklungspraktiken**: Unser sicherer Softwareentwicklungslebenszyklus umfasst Schwachstellenanalysen, kontinuierliche Überwachung und automatisierte Sicherheitsscans, um Sicherheitslücken zu erkennen und zu beheben.
- **Regelmäßige Sicherheitsaudits**: Wir führen sowohl interne als auch externe Audits durch, um die Einhaltung der Vorschriften sicherzustellen und Sicherheitsrisiken proaktiv zu begegnen.
- **SIEM mit Azure Sentinel**: Wir verwenden Azure Sentinel für die Echtzeit-Erkennung von Bedrohungen, automatisierte Reaktionen und die kontinuierliche Sicherheitsüberwachung in allen Cloud- und Netzwerkumgebungen.

Durch die Implementierung dieser Sicherheitsmaßnahmen stärkt MyQ Roger sein gesamtes Sicherheitsframework und stellt sicher, dass Kundendaten jederzeit geschützt bleiben.

4.6 Microsoft Azure und Compliance

MyQ Roger läuft auf Microsoft Azure und nutzt Azure Kubernetes Service (AKS), Azure SQL Server und Azure Cosmos DB für MongoDB. Durch den Betrieb innerhalb der Azure-Infrastruktur profitieren wir von den branchenführenden Sicherheits-, Compliance- und Zuverlässigkeitsstandards von Microsoft.

4.6.1 Sicherheits- und Compliance-Verantwortlichkeiten von Microsoft

- Azure hält sich an globale Compliance-Rahmenwerke wie ISO 27001, SOC 2 und DSGVO in der EU und gewährleistet so die Einhaltung strenger regulatorischer Standards.
- Microsoft bietet integrierte Sicherheitsfunktionen wie Netzwerkisolierung, Identitätsschutz und kontinuierliche Bedrohungserkennung, wodurch Angriffsflächen reduziert werden.
- Azure-Dienste werden strengen Sicherheitsbewertungen und Penetrationstests unterzogen, um Schwachstellen proaktiv zu identifizieren und zu beheben.

Durch die Nutzung der sicheren Infrastruktur von Azure fügt MyQ Roger eigene Sicherheitsebenen hinzu, um ein robustes und widerstandsfähiges Sicherheitsmodell zu schaffen, das Kundenanwendungen und -daten schützt.

4.7 Sicherheitsverantwortlichkeiten der Kunden

MyQ Roger bietet zwar eine sichere Infrastruktur und erstklassige Sicherheitsmaßnahmen, aber auch Kunden haben wichtige Verantwortlichkeiten, um die Sicherheit ihrer Umgebung zu gewährleisten. Dazu gehören:

- **Führen einer Liste aktiver Benutzer**: Kunden sollten den Benutzerzugriff kontinuierlich verwalten, indem sie die automatische Benutzersynchronisierung nutzen oder inaktive Konten manuell deaktivieren, um das Risiko zu minimieren.
- **Durchsetzung der rollenbasierten Zugriffskontrolle (RBAC)**: Kunden müssen RBAC-Prinzipien anwenden, um den Benutzerzugriff auf die erforderlichen Berechtigungen zu beschränken und so eine höhere Sicherheit und Betriebseffizienz zu gewährleisten.
- **Sicherung des lokalen Netzwerks**: Auch wenn MyQ Roger mit einem Zero-Trust-Modell arbeitet, sollten Kunden sicherstellen, dass ihr lokales Netzwerk den besten Sicherheitspraktiken entspricht, wie z. B. Firewall-Konfigurationen, Netzwerksegmentierung und Endpunktschutz.
- **Ordnungsgemäße Wartung der Ressourcen**: Alle angeschlossenen Geräte, einschließlich Drucker und Multifunktionsgeräte (MFPs), sollten regelmäßig mit der neuesten Firmware und Sicherheitspatches aktualisiert werden, um Schwachstellen zu vermeiden.

Durch die Einhaltung dieser Verantwortlichkeiten stärken Kunden ihre Sicherheitslage und profitieren gleichzeitig vom umfassenden Sicherheitsframework von MyQ Roger.

4.8 Sicherheitsautomatisierung

Um die Sicherheit während des gesamten Entwicklungszyklus weiter zu verbessern, integriert MyQ Roger automatisierte Sicherheitstests und externe Sicherheitsbewertungen:

- **SAST (Static Application Security Testing)**: Wird bei jedem Commit durchgeführt, um Sicherheitslücken frühzeitig im Entwicklungszyklus zu erkennen und so die Wahrscheinlichkeit zu verringern, dass unsicherer Code in die Produktion gelangt.

- **DAST (Dynamic Application Security Testing)**: Wird in Sandbox-Umgebungen durchgeführt, um Sicherheitsrisiken während der Laufzeit vor der Bereitstellung zu identifizieren und zu mindern.
- **Externe Penetrationstests**: Wir beauftragen unabhängige Sicherheitsexperten mit der Durchführung von Penetrationstests, um sicherzustellen, dass unsere Sicherheitsvorkehrungen realen Angriffsszenarien standhalten können.

Durch die Automatisierung von Sicherheitstests und die Durchführung regelmäßiger externer Bewertungen gewährleistet MyQ Roger eine proaktive und widerstandsfähige Sicherheitsstrategie.

4.9 Fazit

Bei MyQ Roger ist Sicherheit kein nachträglicher Gedanke, sondern ein integraler Bestandteil unseres Produkt- und Entwicklungslebenszyklus. Durch die Kombination von Secure-by-Design-Prinzipien, bewährten Branchenverfahren und einem starken Compliance-Rahmen bieten wir eine robuste Sicherheitsstrategie, die die Daten und Abläufe unserer Kunden schützt. Unser Engagement für kontinuierliche Sicherheitsverbesserungen stellt sicher, dass MyQ Roger gegenüber sich entwickelnden Bedrohungen widerstandsfähig bleibt und gleichzeitig die höchsten Standards in Bezug auf Zuverlässigkeit und Vertrauen aufrechterhält. Wir werden unsere Sicherheitsstrategie weiterentwickeln, uns an neue Herausforderungen anpassen und die neuesten Technologien nutzen, um unsere Mission zu erfüllen, eine sichere und nahtlose Benutzererfahrung zu bieten.

5 Datenschutz

5.1 Übersicht

Der Datenschutz steht im Mittelpunkt des Sicherheitsansatzes **von MyQ Roger** und stellt sicher, dass jeder Aspekt der cloudbasierten Druck- und Scanlösung den höchsten Industriestandards entspricht. Ein Grundprinzip von MyQ Roger ist, dass **keine Druck- oder Scanauftragsdaten über seine Server übertragen werden**. Stattdessen beschränkt MyQ Roger die Datenerfassung streng auf wesentliche **Metadaten** wie **Auftragsdateinamen, Dateigrößen und Informationen zur Seitenanzahl**. Dies gewährleistet betriebliche Effizienz und schützt gleichzeitig die Privatsphäre der Benutzer.

5.2 Multi-Tenant-Cloud-Sicherheit

Als **Multi-Tenant-Cloud-Produkt** bietet MyQ Roger seinen Kunden eine **logisch isolierte** Umgebung, um eine Datenoffenlegung zwischen verschiedenen Mandanten zu verhindern.

Um Ausfallsicherheit zu gewährleisten, setzt MyQ Roger auf **Azure SQL** und **Azure Cosmos DB**, die beide über integrierte Sicherheitsfunktionen wie **Datenverschlüsselung im Ruhezustand und während der Übertragung, automatische Erkennung von Bedrohungen und Zugriffsüberwachung** verfügen. Die Cloud-Infrastruktur wird kontinuierlichen Sicherheitsbewertungen unterzogen**,** um die mit Multi-Tenant-Umgebungen verbundenen Risiken zu minimieren.

5.3 Verschlüsselung und sichere Kommunikation

Sicherheit ist in alle Ebenen des Betriebs von MyQ Roger integriert. Die gesamte Kommunikation zwischen Clients, Cloud-Diensten und Druckern wird **mit TLS (Transport Layer Security) verschlüsselt**, um unbefugten Zugriff oder Manipulationen zu verhindern.

Um die Sicherheit weiter zu erhöhen, werden alle in MyQ Roger verwendeten Zertifikate von **öffentlich vertrauenswürdigen Zertifizierungsstellen (CAs)** signiert, wodurch ein Höchstmaß an Vertrauen gewährleistet wird. Darüber hinaus werden die Zertifikate **alle drei Monate ausgetauscht**, wodurch das Risiko einer möglichen Kompromittierung verringert und die Einhaltung der besten Sicherheitspraktiken gewährleistet wird.

5.4 Compliance und Identitätsmanagement

MyQ Roger entspricht international anerkannten Sicherheitsstandards und verfügt über **die ISO 27001-Zertifizierung**, was sein Engagement für die Umsetzung robuster Praktiken im Bereich des Informationssicherheitsmanagements unterstreicht.

Um strenge Zugriffskontrollen durchzusetzen, wird **eine rollenbasierte Zugriffskontrolle (RBAC)** implementiert, die sicherstellt, dass Benutzer **nur die für ihre Rolle erforderlichen Berechtigungen** erhalten. Dadurch wird der Zugriff auf sensible Daten minimiert und das Risiko eines versehentlichen oder vorsätzlichen Missbrauchs verringert.

5.5 DSGVO-Konformität

Die Einhaltung der **Datenschutz-Grundverordnung (DSGVO)** hat für MyQ Roger höchste Priorität. In Übereinstimmung mit den Grundsätzen der DSGVO befolgt MyQ Roger strenge Datenschutzmaßnahmen, um die Privatsphäre der Benutzer zu schützen:

- **Datenminimierung**: Es werden nur wesentliche Metadaten erfasst, wodurch das Risiko der Speicherung sensibler Benutzerdokumente ausgeschlossen wird.
- **Benutzerrechte und -kontrolle**: Benutzer haben die Möglichkeit**,** gemäß der DSGVO **Zugriff** auf ihre personenbezogenen Daten zu beantragen**, diese zu korrigieren, zu löschen oder zu anonymisieren**.
- **Transparenz bei der Datenverarbeitung**: Klare und prägnante Datenschutzrichtlinien beschreiben, wie Metadaten behandelt, gespeichert und geschützt werden.
- **Sichere Datenspeicherung**: Alle Daten werden **im Ruhezustand und während der Übertragung verschlüsselt**, wodurch die vollständige Einhaltung der strengen Sicherheitsanforderungen der DSGVO gewährleistet ist.
- **Anonymisierungsmaßnahmen**: Bei Bedarf setzt MyQ Roger **Datenanonymisierungstechniken** ein, um sicherzustellen, dass personenbezogene Daten nicht mehr einem bestimmten Benutzer zugeordnet werden können, wodurch der Datenschutz verstärkt wird.

Diese Maßnahmen stellen sicher, dass MyQ Roger die Kernanforderungen der DSGVO vollständig erfüllt und den Benutzern die Kontrolle über ihre personenbezogenen Daten gibt, während gleichzeitig eine sichere und konforme Umgebung gewährleistet ist.

5.6 Datensicherungen

Zum Schutz vor Datenverlust und zur Gewährleistung der Zuverlässigkeit des Dienstes implementiert MyQ Roger eine **umfassende Datensicherungsstrategie**. Diese umfasst:

- **Automatisierte Backups**: Regelmäßig geplante **inkrementelle und vollständige Backups** stellen sicher, dass Daten im Falle eines Vorfalls wiederhergestellt werden können.
- **Sichere Speicherung**: Backups werden mit **AES-256-Verschlüsselung** verschlüsselt, sodass die Daten selbst im unwahrscheinlichen Fall eines unbefugten Zugriffs unlesbar bleiben.
- **Aufbewahrungsrichtlinien**: Backups werden **für einen festgelegten Zeitraum** in Übereinstimmung mit den Compliance-Anforderungen **gespeichert**, was eine effiziente Wiederherstellung im Falle eines Systemausfalls oder einer Notfallwiederherstellung ermöglicht.
- **Integritätsprüfung und -verifizierung**: Es werden regelmäßig **Integritätsprüfungen der Backups** durchgeführt, um sicherzustellen, dass die gespeicherten Backups funktionsfähig und zuverlässig sind und bei Bedarf eine nahtlose Datenwiederherstellung gewährleisten.

Durch die Implementierung dieser robusten Sicherheits-, Compliance- und Backup-Maßnahmen **bietet MyQ Roger eine sichere, private und hocheffiziente Cloud-basierte Druck- und Scan-Lösung**, die den höchsten Datenschutzstandards der Branche entspricht.

6 Datenschutzrichtlinie

Der Schutz Ihrer Daten ist uns wichtig, und wir nehmen ihn sehr ernst. Diese Datenschutzerklärung für MyQ Roger Solution (die „Datenschutzerklärung“) erläutert, welche Art von Informationen MyQ im Zusammenhang mit der Bereitstellung von Produkten, Dienstleistungen, Inhalten, Anwendungen oder anderen Komponenten, die Teil der MyQ Roger Solution sind (die „Dienste“), erfassen, speichern und verarbeiten kann und wie diese Informationen verwendet und geschützt werden. Außerdem wird dargelegt, wie Sie uns kontaktieren können, wenn Sie Fragen oder Bedenken bezüglich Ihrer personenbezogenen Daten haben.

Diese Datenschutzerklärung wird herausgegeben von MyQ, spol. s.r.o., mit Sitz in Českomoravská 2420/15, Libeň, 190 00 Praha 9, Tschechische Republik, Firmen-ID-Nr. 615 06 133, eingetragen im Handelsregister des Stadtgerichts in Prag, Abschnitt C, Eintrag 29842 („MyQ“ oder „wir“).

Wir behalten uns das Recht vor, diese Datenschutzerklärung jederzeit zu ändern. Bitte überprüfen Sie die Datenschutzerklärung regelmäßig auf Änderungen. Wenn Sie unser Kunde sind, können wir Sie jedoch auch per E-Mail über Änderungen informieren, die nach unserem alleinigen Ermessen wesentliche Auswirkungen auf Ihre Nutzung der Dienste oder die Art und Weise haben, wie wir Ihre personenbezogenen Daten verarbeiten. Durch Ihre fortgesetzte Nutzung unserer Dienste, die unter diese Datenschutzerklärung fallen, erklären Sie sich mit allen Änderungen einverstanden, die wir von Zeit zu Zeit an dieser Datenschutzerklärung vornehmen.

6.1 1. Daten, die wir erfassen oder erhalten

Wir erfassen personenbezogene Daten von unseren Kunden als Nutzern der Dienste und deren Endnutzern (einschließlich der Mitarbeiter unserer Kunden), um Benutzerkonten einzurichten und zu verwalten sowie die Dienste bereitzustellen und zu verwalten. Wir erfassen auch Nutzungsdaten und Metriken. Wir sind der Datenverantwortliche in Bezug auf diese personenbezogenen Daten.

In Bezug auf personenbezogene Daten, die in den Metadaten der Inhalte enthalten sein können, wie in den Nutzungsbedingungen https://www.myq-solution.com/en/myq-legal-documents definiert, die die Nutzer oder Endnutzer mithilfe der Dienste verwalten, oder in Bezug auf personenbezogene Daten, auf die wir während der Bereitstellung von Remote- oder lokalen Supportdiensten Zugriff haben (die „Kundendaten“), verarbeiten wir diese personenbezogenen Daten im Auftrag

unserer Kunden als Datenverarbeiter. Wenn wir die Kundendaten verarbeiten, um unseren Kunden die Dienste bereitzustellen, handeln wir gemäß den Anweisungen unserer Kunden als deren Datenverarbeiter. Wir bewahren die Kundendaten, die wir im Auftrag unserer Kunden und gemäß deren Anweisungen verarbeiten, stets getrennt von den Daten unserer anderen Kunden auf und behandeln sie streng vertraulich.

6.1.1 1.1 Daten von Nutzern und Endnutzern unserer Dienste

Wir erfassen Ihre personenbezogenen Daten, wenn:

- Sie ein Konto innerhalb unserer Dienste erstellen;
- Sie sich bei unserem Dienst anmelden, indem Sie Ihren Benutzernamen (E-Mail-Adresse) und Ihr Passwort eingeben;
- Sie unsere Dienste nutzen oder anderweitig mit MyQ interagieren, beispielsweise wenn Sie Anfragen an uns richten;
- Sie MyQ solche Daten auf andere Weise freiwillig zur Verfügung stellen.

Wenn Sie ein Konto bei MyQ erstellen, bitten wir Sie, ein Registrierungsformular auszufüllen, in dem Sie Ihren Vornamen, Nachnamen, Ihre E-Mail-Adresse, Ihr Unternehmen und Ihre Berufsbezeichnung angeben. Sie können Ihrem Konto auch eine Telefonnummer hinzufügen.

Wir erfassen und verarbeiten auch Ihren Benutzernamen (E-Mail-Adresse) und Ihr Passwort.

Zum Zwecke der Analyse und Verbesserung unserer Dienste können unsere Server automatisch Informationen aufzeichnen, wenn Sie unsere Website besuchen oder einige unserer Dienste nutzen („Nutzungsdaten“), darunter:

- Informationen über Dienste von Drittanbietern, die der Nutzer und seine Endnutzer zu Authentifizierungszwecken und zur Verbindung mit dem Cloud-Speicher des Nutzers mit den Diensten verbinden;
- Informationen über die Geräte des Benutzers, z. B. Typ und Marke der Drucker und deren Seriennummer;
- Informationen über die Nutzung unserer Dienste, z. B. die Anzahl der gedruckten oder gescannten Dokumente.

Die Dienste ermöglichen es Ihnen, eine Verbindung zu Anwendungen von Drittanbietern oder anderen Diensten herzustellen, z. B. One Drive oder Google Disk, um Dokumente und andere Inhalte mit den Diensten zu teilen. Wenn Sie sich für eine Verbindung zu Diensten von Drittanbietern entscheiden, bitten wir Sie um Ihre Zustimmung, damit die Dienste auf diese Dienste von Drittanbietern zugreifen

können. MyQ verarbeitet jedoch keine dort gespeicherten personenbezogenen Daten, mit Ausnahme der oben definierten Kundendaten.

Wenn unsere Dienste von einem Unternehmen erworben werden, sind es die einzelnen Benutzer innerhalb der Organisation dieses Unternehmens, die sich bei unserer Dienstplattform anmelden und deren personenbezogene Daten wie oben beschrieben erfasst werden. Wenn ein solches Unternehmen uns direkt personenbezogene Daten seiner Mitarbeiter oder anderer einzelner Benutzer, denen es den Zugriff auf die Dienste gestattet hat, zur Verfügung stellt, muss es über alle erforderlichen Einwilligungen, Genehmigungen oder Registrierungen verfügen, um die personenbezogenen Daten seiner Mitarbeiter oder Benutzer zu verarbeiten und uns zur Verfügung zu stellen.

6.1.2 1.2 Kundendaten

Um unseren Nutzern und Endnutzern unsere Dienste bereitzustellen, können wir auch Kundendaten im oben definierten Sinne verarbeiten. Die Verarbeitung von Kundendaten unterliegt der Datenschutzerklärung der Nutzer, und die Nutzer sind verpflichtet, sicherzustellen, dass die Verarbeitung dieser Daten rechtmäßig ist und den geltenden Gesetzen entspricht. Die Verarbeitung von Kundendaten durch MyQ wird durch geltende Datenverarbeitungsvereinbarungen mit den Nutzern geregelt.

6.2 2. Wie wir die Daten verwenden

Wir verwenden Ihre personenbezogenen Daten für die folgenden Zwecke:

6.2.1 2.1 Zur Bereitstellung der Dienste

Wir können Ihre personenbezogenen Daten verarbeiten, um Sie zu identifizieren, wenn Sie sich bei Ihrem Konto anmelden und unsere Dienste nutzen, damit wir die Dienste betreiben und Ihnen zur Verfügung stellen können. Dies kann die Überprüfung Ihrer Zahlungen, Bestellungen und Rechnungsdaten umfassen.

6.2.2 2.2 Zur Kommunikation mit Ihnen

Wir können Daten unserer Kunden oder ihrer einzelnen Endnutzer, insbesondere E-Mail-Adressen oder andere Kontaktdaten, verarbeiten, um mit unseren Nutzern und Endnutzern zu kommunizieren, beispielsweise wenn wir ihnen bei der Einrichtung oder Verwaltung ihres Kontos helfen, wenn wir Kundendienst und Support leisten, technische Mitteilungen, Updates zu bevorstehenden Änderungen oder

Verbesserungen der Dienste, Erinnerungen, Sicherheitswarnungen und andere Support- und Verwaltungsnachrichten versenden.

6.2.3 2.3 Um eine bessere Benutzererfahrung zu bieten

Wir können Ihre personenbezogenen Daten verarbeiten, um zu erfahren, wie Sie unsere Dienste nutzen, und dadurch die Benutzererfahrung kontinuierlich zu verbessern sowie einen nahtlosen Kundenservice zu bieten. Wir können solche personenbezogenen Daten auch verarbeiten, um unsere bestehenden Dienste zu verbessern und zu erweitern und neue Angebote zu entwickeln. Dazu gehören Produkt- und Marktstatistiken, Forschung und Analysen, Benchmarks und andere Analysen, um Ihre Bedürfnisse und die Bedürfnisse der Nutzer insgesamt besser zu verstehen, Probleme zu diagnostizieren und Trends zu analysieren.

6.2.4 2.4 Zum Schutz unserer Dienste und zur Verteidigung unserer Rechte oder der Rechte Dritter

Wir verarbeiten Ihre personenbezogenen Daten, um die Sicherheit und Zuverlässigkeit der Dienste zu gewährleisten. Dazu gehören die Erkennung, Verhinderung und Bekämpfung von Betrug, Missbrauch, Sicherheitsrisiken und technischen Problemen, die MyQ, unseren Kunden und Endnutzern schaden könnten.

Wir können einige der in Abschnitt 1.1 genannten Daten verarbeiten, wenn dies gesetzlich vorgeschrieben ist oder um unsere Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen oder, falls erforderlich, die Rechte und Interessen von MyQ zu schützen.

6.2.5 2.5 Zu Marketing- und Vertriebszwecken

Wir können die Kontaktdaten der von Ihnen oder Ihren Endnutzern benannten Ansprechpartner verarbeiten, um Ihnen Informationen über neue Funktionen der Dienste und neue Produktangebote zukommen zu lassen. Weitere Einzelheiten finden Sie in Abschnitt 7 unten.

6.3 3. Rechtsgrundlage

Für die in den Abschnitten 2.1 und 2.2 genannten Zwecke verarbeiten wir Ihre personenbezogenen Daten auf der Grundlage unseres Vertrags mit Ihnen (wenn Sie unser direkter Kunde und eine natürliche Person sind) oder auf der Grundlage unseres berechtigten Interesses, unseren Kunden unsere Dienste anzubieten (wenn

unser Kunde Ihr Unternehmen oder Ihre Organisation ist und Sie ein von Ihrem Unternehmen oder Ihrer Organisation benannter autorisierter Endnutzer sind).

Für die in Abschnitt 2.3 genannten Zwecke verarbeiten wir Ihre personenbezogenen Daten auf der Grundlage unseres berechtigten Interesses an der Entwicklung und Verbesserung unserer Dienste.

Für die in Abschnitt 2.4 genannten Zwecke verarbeiten wir Ihre personenbezogenen Daten auf der Grundlage unseres berechtigten Interesses, unsere Rechte oder Ansprüche oder die Rechte unserer Kunden oder Nutzer zu schützen und zu sichern.

Für die in Abschnitt 2.5 genannten Zwecke verarbeiten wir Ihre personenbezogenen Daten auf der Grundlage Ihrer freiwilligen Einwilligung, sofern Sie uns diese Einwilligung erteilt haben. In einem nach geltendem Recht zulässigen begrenzten Umfang können wir Ihre elektronischen Kontaktdaten auch ohne Ihre ausdrückliche Einwilligung auf der Grundlage unseres berechtigten Interesses verwenden, um Sie über unsere Dienste zu informieren, wie in Abschnitt 7 unten näher beschrieben.

Wenn wir Ihre personenbezogenen Daten für unsere berechtigten Interessen verwenden, stellen wir sicher, dass wir alle potenziellen Auswirkungen berücksichtigen, die eine solche Verwendung auf Sie haben könnte. Unsere berechtigten Interessen haben nicht automatisch Vorrang vor Ihren Interessen, und wir verwenden Ihre Daten nicht, wenn wir der Ansicht sind, dass Ihre Interessen Vorrang vor unseren Interessen haben sollten, es sei denn, wir haben andere Gründe dafür (z. B. die Erfüllung eines Vertrags, Ihre Einwilligung oder eine gesetzliche Verpflichtung). Wenn Sie Bedenken hinsichtlich unserer Verarbeitung haben, lesen Sie bitte die Details zu „Ihren Rechten" in Abschnitt 9 unten.

6.4 4. Aufbewahrungsfristen

Wenn wir personenbezogene Daten als Datenverantwortlicher verarbeiten, speichern wir Ihre personenbezogenen Daten für den Zeitraum, der zur Erfüllung der in dieser Datenschutzerklärung und/oder einer Vereinbarung über Dienste genannten Zwecke erforderlich ist, es sei denn, eine längere Aufbewahrung ist gesetzlich vorgeschrieben (z. B. für Steuer- oder Buchhaltungszwecke oder aufgrund anderer gesetzlicher Anforderungen) oder die Speicherung der Daten ist für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen von MyQ erforderlich. In diesem Fall speichern wir nur die Daten, die für die Durchsetzung unserer Ansprüche oder unsere Verteidigung erforderlich sind, und zwar für den im jeweiligen Fall erforderlichen Zeitraum und nicht länger als die gesetzlichen Verjährungsfristen.

Wenn wir personenbezogene Daten im Auftrag unserer Kunden als Datenverarbeiter verarbeiten, speichern wir diese Daten für die Dauer unserer Vereinbarung mit diesen Kunden und löschen sie gemäß unseren Aufbewahrungs- und Sicherungsprozessen automatisch innerhalb von 90 Tagen nach Beendigung der Vereinbarung, es sei denn, die Kunden bitten uns, sie früher zu löschen.

6.5 5. Weitergabe Ihrer personenbezogenen Daten für rechtliche und geschäftliche Zwecke

Wir können Informationen über Sie verwenden und/oder an Dritte (einschließlich Regierungsbehörden und Strafverfolgungsbehörden, unsere verbundenen Unternehmen, professionelle Berater und unsere Lieferanten oder Subunternehmer) weitergeben, wenn:

- Einhaltung rechtlicher Verfahren;
- die gesetzlichen Rechte von MyQ durchsetzen oder verteidigen und im Zusammenhang mit einer Unternehmensumstrukturierung wie einer Fusion, einer Unternehmensübernahme oder einer Insolvenz;
- Verhinderung von Betrug oder drohendem Schaden; und
- die Sicherheit und Funktionsfähigkeit unseres Netzwerks und unserer Dienste gewährleisten.

Diese Informationen werden weitergegeben, vorausgesetzt, dass wir in allen diesen Fällen nur die begrenzten personenbezogenen Daten weitergeben, die in der jeweiligen Situation erforderlich sind.

Wir geben Ihre Daten an unsere vertrauenswürdigen Geschäftspartner oder Personen weiter, die Ihre Daten als unsere Datenverarbeiter in unserem Auftrag und gemäß unseren Anweisungen in Übereinstimmung mit dieser Datenschutzrichtlinie verarbeiten. Wir wählen unsere Lieferanten sehr sorgfältig aus und stellen stets sicher, dass sie angemessene Datenschutz- und Sicherheitsvorkehrungen treffen. Zu diesem Zweck haben wir unsere Datenverarbeiter an Datenverarbeitungsvereinbarungen gebunden, die gemäß Artikel 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) („DSGVO“)

Wenn Sie in der MyQ-Verwaltungsoberfläche einen Dienst in der EU auswählen, werden Ihre Kundendaten gemäß den vertraglichen Verpflichtungen von Microsoft zur EU-Datengrenze in der EU verarbeitet. Wenn Sie in der MyQ-

Verwaltungsoberfläche einen Dienst außerhalb der EU auswählen, erfolgt diese Übertragung auf der Grundlage der von der Europäischen Kommission genehmigten Standardvertragsklauseln (Musterklauseln) (2010/87/EU), sofern kein anderer Übertragungsmechanismus gemäß Artikel 45, 46 ff. der DSGVO verfügbar ist. Ungeachtet des Vorstehenden können Ihre Kundendaten auch in Länder übertragen werden, für die die Europäische Kommission eine Angemessenheitsentscheidung getroffen hat.

Die Liste unserer aktuellen Auftragsverarbeiter, die Zugriff auf Ihre personenbezogenen Daten haben können:

- http://salesforce.comEMEA Ltd. (vertriebsbezogene Verarbeitung und technischer Support),
- Microsoft Ireland Operations Limited (Zusammenarbeit und Kommunikation, Microsoft Azure – Cloud-Hosting-Dienste),
- TeamViewer GmbH (technischer Support).

Neben den oben genannten Auftragsverarbeitern können wir Ihre personenbezogenen Daten auch weitergeben, um unsere Geschäftsprozesse zu verwalten und unseren gesetzlichen Verpflichtungen nachzukommen, einschließlich logistischer, abrechnungstechnischer, steuerlicher, rechtlicher und technischer Dienste.

Neben Drittanbietern kann MyQ Daten an seine verbundenen Unternehmen in der EU und im Vereinigten Königreich weitergeben, um bestimmte logistische, abrechnungsbezogene, steuerliche, rechtliche und technische Dienste zu erbringen. Die aktualisierte Liste unserer verbundenen Unternehmen in der EU und im Vereinigten Königreich finden Sie unter https://www.myq-solution.com/en/the-list-of-myq-data-processors .

6.6 6. Anonyme Statistiken

Wir können aggregierte anonymisierte Daten, die aus den von Ihnen bereitgestellten personenbezogenen Daten oder durch Programmanalysen wie Benutzerverhalten und -aktivitäten gewonnen wurden, für unsere eigenen Statistiken, für Audits, für Produkt- und Marktforschung, für Analysen (die uns helfen, unsere Dienste und deren Benutzerfreundlichkeit sowie das Dienstleistungsangebot zu optimieren und zu verbessern und neue Technologien, Produkte und Dienste zu entwickeln) sowie für Benchmarks und andere Analysen verwenden.

6.7 7. Marketingmitteilungen

Wir können die von Ihnen oder Ihren Endnutzern benannten Ansprechpartner kontaktieren, um Informationen zu neuen Funktionen der Dienste und neuen Produktangeboten bereitzustellen, sofern wir die erforderliche Erlaubnis dazu haben, entweder auf der Grundlage Ihrer Einwilligung (sofern wir diese angefordert haben und Sie uns diese erteilt haben) oder aufgrund unserer berechtigten Interessen, Ihnen Marketingmitteilungen zuzusenden, sofern wir dies rechtmäßig tun dürfen, innerhalb der gesetzlich vorgesehenen Grenzen. Im letzteren Fall senden wir Ihnen nur dann Marketingmitteilungen zu, wenn Sie einen unserer Dienste nutzen oder kürzlich genutzt haben und dem Erhalt solcher Informationen nicht widersprochen haben (auf eine der unten genannten Weisen).

Ihre Präferenzen für Marketingmitteilungen können jederzeit geändert werden, indem Sie die folgenden Anweisungen befolgen:

- Wenn Sie sich von einer Ihnen zugesandten E-Mail abmelden möchten, folgen Sie dem Link „Abmelden“ und/oder den Anweisungen am Ende der E-Mail.
- Alternativ können Sie uns über die Angaben im Abschnitt „Kontakt” unten kontaktieren, um Ihre Präferenzen für Marketingmitteilungen zu ändern, einschließlich des Widerrufs Ihrer Einwilligung.

Wenn Sie unerwünschte, unaufgeforderte E-Mails erhalten haben, die über unser System versendet wurden oder angeblich über unser System versendet wurden, leiten Sie bitte eine Kopie dieser E-Mail mit Ihren Kommentaren zur Überprüfung an info@myq-solution.com[1] weiter.

Bitte beachten Sie, dass wir Ihnen gelegentlich wichtige Informationen (auch per E-Mail) über unsere Dienste senden können, die Sie nutzen oder genutzt haben, einschließlich Änderungen der geltenden Geschäftsbedingungen und/oder anderer Mitteilungen oder Benachrichtigungen, die zur Erfüllung unserer gesetzlichen und vertraglichen Verpflichtungen erforderlich sind, wie in Abschnitt 2.2 oben beschrieben. Diese wichtigen Dienstmitteilungen stellen keine Marketingmitteilungen dar und sind von Ihren Präferenzen nicht betroffen.

6.8 8. Sicherheit und Speicherort Ihrer Daten

Wir haben angemessene technische und organisatorische Maßnahmen, interne Kontrollen und Routinen zur Informationssicherheit in Übereinstimmung mit den bewährten Verfahren der Branche und unter Berücksichtigung des Stands der

1. mailto:info@myq-solution.com

technologischen Entwicklung implementiert und werden diese aufrechterhalten, um Ihre Daten vor versehentlichem Verlust, Zerstörung, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff oder unrechtmäßiger Zerstörung zu schützen. Zu diesen Maßnahmen können unter anderem gehören: angemessene Schritte zur Sicherstellung der Zuverlässigkeit der Mitarbeiter, die Zugriff auf Ihre Daten haben, und die Gewährung begrenzter Zugriffsrechte und Zugriffskontrollen; Authentifizierung; Schulung des Personals; regelmäßige Datensicherung; Verfahren zur Datenwiederherstellung und zum Vorfallsmanagement; Beschränkungen für die Speicherung, den Ausdruck und die Entsorgung personenbezogener Daten; Softwareschutz für Geräte, auf denen personenbezogene Daten gespeichert sind; usw.

6.9 9. Ihre Rechte

In diesem Abschnitt werden Ihre Rechte gemäß den geltenden Gesetzen, wie z. B. der DSGVO, und deren Anwendung beschrieben. Wenn Sie eines Ihrer Rechte gemäß diesem Abschnitt oder gemäß den geltenden Gesetzen ausüben, werden wir jede Berichtigung oder Löschung Ihrer personenbezogenen Daten oder jede Einschränkung der Verarbeitung, die gemäß Ihrer Anfrage durchgeführt wurde, jedem Empfänger mitteilen, dem die personenbezogenen Daten gemäß Abschnitt 5 dieser Datenschutzerklärung offengelegt wurden, es sei denn, eine solche Mitteilung erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Wenn Sie diese Rechte ausüben und/oder alle relevanten Informationen über die Verarbeitung Ihrer personenbezogenen Daten erhalten möchten, kontaktieren Sie uns bitte unter info@myq-solution.com[2]. Sie werden gebeten, sich zu identifizieren; dies ist notwendig, um zu überprüfen, ob die Anfrage von Ihnen gesendet wurde. Wir werden innerhalb eines Monats nach Eingang Ihrer Anfrage antworten, behalten uns jedoch das Recht vor, diese Frist in begründeten Ausnahmefällen auf bis zu zwei Monate zu verlängern. Wir werden Sie in jedem Fall innerhalb eines Monats nach Eingang Ihrer Anfrage informieren, wenn wir beschließen, die Frist für unsere Antwort zu verlängern.

In Übereinstimmung mit den geltenden Gesetzen und wie nachstehend näher beschrieben, haben Sie das Recht, Zugang zu Ihren personenbezogenen Daten und Informationen über deren Verarbeitung zu verlangen, das Recht auf Berichtigung, Löschung oder Übertragbarkeit (z. B. Übertragung Ihrer personenbezogenen Daten

2. mailto:info@myq-solution.com

an einen anderen Dienstleister) Ihrer von uns verarbeiteten personenbezogenen Daten sowie das Recht, der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen und/oder eine Einschränkung dieser Verarbeitung zu verlangen.

Bitte beachten Sie, dass Ihr Widerspruch gegen die Verarbeitung dazu führen kann, dass wir Ihnen unsere Dienste nicht mehr anbieten oder die zur Erreichung der oben genannten Zwecke erforderlichen Maßnahmen nicht mehr durchführen können (siehe Abschnitt 2 „Wie wir die Daten verwenden“).

Es ist wichtig, dass die personenbezogenen Daten, die wir über Sie gespeichert haben, korrekt und aktuell sind. Bitte informieren Sie uns, wenn sich Ihre personenbezogenen Daten während Ihrer Beziehung zu uns ändern, indem Sie uns über die Kontaktdaten in Abschnitt 10 „Kontakt“ kontaktieren.

6.9.1 9.1 Informationen über Ihre personenbezogenen Daten, Zugriff darauf und Berichtigung

Gemäß den geltenden Gesetzen haben Sie das Recht, eine Bestätigung darüber zu erhalten, ob personenbezogene Daten über Sie verarbeitet werden (gemäß dem oben beschriebenen Verfahren), und, falls dies der Fall ist, das Recht auf Zugang zu Ihren personenbezogenen Daten, die Sie uns mitgeteilt haben, und auf deren Berichtigung. Über Ihre Einstellungen in den Diensten können Sie auf Ihre Kontoinformationen zugreifen, diese aktualisieren und Ihre Profileinstellungen ändern.

6.9.2 9.2 Richtigkeit Ihrer personenbezogenen Daten

Wir ergreifen angemessene Maßnahmen, um sicherzustellen, dass Sie Ihre personenbezogenen Daten korrekt und aktuell halten können. Sie können sich jederzeit an uns wenden, um eine Bestätigung darüber zu erhalten, ob wir Ihre personenbezogenen Daten noch verarbeiten.

Wenn Sie feststellen, dass Ihre von uns verarbeiteten personenbezogenen Daten unrichtig oder unvollständig sind und Sie Ihre personenbezogenen Daten nicht gemäß Abschnitt 9.1 dieser Datenschutzerklärung aktualisieren können, können Sie uns auffordern, diese personenbezogenen Daten zu aktualisieren. Wir werden Ihre Identität überprüfen und Ihre personenbezogenen Daten in Ihrem Namen aktualisieren.

6.9.3 9.3 Löschung Ihrer personenbezogenen Daten

Sie können uns jederzeit auffordern, Ihre personenbezogenen Daten zu löschen. Wenn Sie uns mit einer solchen Anfrage kontaktieren, werden wir alle Ihre personenbezogenen Daten, über die wir verfügen, unverzüglich löschen, sofern Ihre personenbezogenen Daten nicht mehr für die Erbringung der Dienste oder andere zulässige Zwecke erforderlich sind, insbesondere im Zusammenhang mit der Ausübung und Verteidigung unserer gesetzlichen Rechte oder der Erfüllung unserer gesetzlichen Verpflichtungen. Wir werden auch alle Ihre personenbezogenen Daten löschen (und die Löschung durch die von uns beauftragten Auftragsverarbeiter sicherstellen), falls Sie Ihre Einwilligung widerrufen oder wenn wir gesetzlich dazu verpflichtet sind.

6.9.4 9.4 Einschränkung der Verarbeitung

Wenn Sie uns auffordern, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken, z. B. in Fällen, in denen Sie die Richtigkeit, Rechtmäßigkeit oder unsere Notwendigkeit zur Verarbeitung Ihrer personenbezogenen Daten bestreiten, werden wir die Verarbeitung Ihrer personenbezogenen Daten auf das erforderliche Minimum (Speicherung) beschränken und sie gegebenenfalls nur zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen oder, falls erforderlich, zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus anderen begrenzten Gründen, die durch das geltende Recht vorgeschrieben sind, verarbeiten. Wird die Einschränkung aufgehoben und setzen wir die Verarbeitung Ihrer personenbezogenen Daten fort, werden Sie unverzüglich darüber informiert.

6.9.5 9.5 Übertragbarkeit Ihrer personenbezogenen Daten

Sie haben das Recht, die Sie betreffenden personenbezogenen Daten, die Sie uns zur Verfügung gestellt haben, zu erhalten. Wenn Sie uns mit einer solchen Anfrage kontaktieren, werden wir Ihnen Ihre personenbezogenen Daten in einem gängigen und maschinenlesbaren Format unverzüglich nach Eingang Ihrer Anfrage zur Verfügung stellen. Auf Ihren Wunsch hin senden wir Ihre personenbezogenen Daten an einen Dritten (einen anderen Datenverantwortlichen), den Sie in Ihrer Anfrage benennen, sofern diese Anfrage nicht die Rechte oder Freiheiten anderer beeinträchtigt und technisch machbar ist.

6.9.6 9.6 Widerspruch gegen die Verarbeitung

Sie haben das Recht, der Verwendung Ihrer personenbezogenen Daten auf der Grundlage unserer berechtigten Interessen zu widersprechen. In diesem Fall werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende berechtigte Gründe für die weitere Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung unserer Rechtsansprüche. Wenn Sie der Verarbeitung Ihrer Daten für Direktmarketingzwecke widersprechen, werden wir Ihre Daten nicht mehr für diese Zwecke verarbeiten.

6.9.7 9.7 Widerruf Ihrer Einwilligung

Wenn Sie uns Ihre Einwilligung zur Verarbeitung personenbezogener Daten erteilt haben, beispielsweise für Marketingkommunikation, können Sie Ihre Einwilligung jederzeit ohne Angabe von Gründen widerrufen. Wir werden Ihre personenbezogenen Daten für jede weitere Verarbeitung sperren. Bitte beachten Sie, dass der Widerruf Ihrer Einwilligung die Rechtmäßigkeit der Verarbeitung auf der Grundlage der Einwilligung vor deren Widerruf nicht beeinträchtigt.

6.9.8 9.8 Beschwerde bei einer Datenschutzbehörde

Sie haben das Recht, eine Beschwerde über unsere Datenverarbeitungsaktivitäten bei Úřad pro ochranu osobních údajů, Pplk. Sochora 2Z, 170 00 Praha 7, Tschechische Republik, einzureichen.

6.9.9 9.9 Antrag auf Widerspruch gegen den Verkauf personenbezogener Daten gemäß dem CCPA

MyQ verkauft keine personenbezogenen Daten im Sinne des CCPA. Wenn ein kalifornischer Verbraucher einen Antrag auf Widerspruch gemäß dieser Bestimmung stellt, hat dieser daher keine Auswirkungen. Wenn Sie weitere Informationen zu Ihren Rechten gemäß dem CCPA zum Widerspruch gegen den Verkauf Ihrer personenbezogenen Daten benötigen, wenden Sie sich bitte an: info@myq-solution.com[3].

3. mailto:info@myq-solution.com

6.10 10. Kontakt

Wenn Sie Fragen zu unseren Praktiken zur Datenerhebung und zum Datenschutz oder zu Ihren Rechten haben, wenden Sie sich bitte an info@myq-solution.com[4].

4. mailto:info@myq-solution.com

7 Server-Betriebszeit, Datensicherung und Disaster Recovery

7.1 Server-Verfügbarkeit

MyQ Roger ist bestrebt, eine Verfügbarkeit von 99,9 % zu gewährleisten. Service Level Agreements (SLAs) werden jedoch individuell auf jeden Kunden zugeschnitten und garantieren diese Kennzahl nicht ausdrücklich. Wir setzen fortschrittliche Hochverfügbarkeitsstrategien (HA) ein und nutzen Multi-Zone-Bereitstellungen und Multi-Pod-Architekturen, um die Kontinuität des Dienstes zu gewährleisten und potenzielle Ausfallzeiten im Falle von Betriebsstörungen zu minimieren.

7.2 Echtzeit-Überwachung des Systemstatus

Um die Transparenz zu verbessern und einen Echtzeit-Einblick in die Systemleistung zu ermöglichen, unterhalten wir eine spezielle Status-Website, die aktuelle Informationen zum Zustand des Dienstes liefert. Diese Plattform ermöglicht Kunden Folgendes:

- **Live-Systemstatus überwachen**: Echtzeit-Betriebsmetriken und Aktualisierungen zu Vorfällen anzeigen.
- **Proaktive Benachrichtigungen erhalten**: Abonnieren Sie Warnmeldungen zu Dienstbeeinträchtigungen oder geplanten Wartungsarbeiten.
- **Auf historische Verfügbarkeitsberichte zugreifen**: Überprüfen Sie vergangene Vorfälle und Leistungstrends, um die Zuverlässigkeit zu bewerten.

Durch die Bereitstellung einer zentralen Status-Website versorgen wir unsere Kunden mit zeitnahen und genauen Informationen, stärken das Vertrauen und ermöglichen proaktive Entscheidungen im Falle von Störungen.

7.3 Sicherungsstrategien

7.3.1 Azure SQL-Sicherungsstrategie

Wir verwenden eine georedundante Sicherungsstrategie für Azure SQL-Datenbanken, um die Ausfallsicherheit und Wiederherstellbarkeit der Daten zu gewährleisten. Zu den wichtigsten Aspekten gehören:

- **Georedundante Speicherung**: Backups werden zur Notfallwiederherstellung über mehrere Regionen hinweg repliziert.
- **Aufbewahrungsrichtlinie**: Backups werden mehrere Monate lang aufbewahrt, sodass historische Daten wiederhergestellt werden können.

- **Inkrementelle Backups**: Ein 14-tägiges Point-in-Time-Recovery-Fenster (PITR) ermöglicht die granulare Wiederherstellung verlorener Daten.
- **SLA-basierte Anpassung**: Aufbewahrungsfristen und Wiederherstellungszeiten (RTO) variieren je nach clusterspezifischen SLAs und können an die Kundenanforderungen angepasst werden.

7.3.2 Azure Cosmos DB-Sicherungsstrategie

Für Azure Cosmos DB implementieren wir umfassende Datenschutzmechanismen, insbesondere für Buchhaltungsunterlagen, um die Datenintegrität und Rückverfolgbarkeit sicherzustellen:

- **Vollständige Buchhaltungsdatenberichte**: Alle Buchhaltungstransaktionen, einschließlich der Jobabrechnung für Druck-, Scan-, Kopier- und Faxaktivitäten, werden vollständig aufgezeichnet.
- **Rückverfolgung historischer Daten**: Unser System ermöglicht die Verfolgung und Rückverfolgung aller gemeldeten Buchhaltungsunterlagen, um Compliance und Überprüfbarkeit sicherzustellen.
- **Hohe Verfügbarkeit und Redundanz**: Die integrierte Replikation über mehrere Regionen hinweg gewährleistet Kontinuität und minimiert das Risiko von Datenverlusten.

Durch die Implementierung dieser robusten Backup-Strategien schützen wir wichtige Geschäftsdaten und bieten gleichzeitig flexible Wiederherstellungsoptionen, die auf kundenspezifische SLAs zugeschnitten sind.

7.4 Katastrophenszenarien und Notfallplan

Katastrophenszenario	Strategie zur Schadensbegrenzung	Wiederherstellungsprozess
Datenbeschädigung	PITR (Point-in-Time Recovery)	Wiederherstellung der Datenbank auf den letzten bekannten fehlerfreien Zustand
Ausfall der Cloud-Region	Georedundante Backups und Failover	Wechsel zur sekundären Azure-Region
Ausfall eines Kubernetes-Knotens	Automatische Replikation von Diensten in AKS	Pods werden auf fehlerfreie Knoten umgeleitet

Katastrophenszenario	Strategie zur Schadensbegrenzung	Wiederherstellungsprozess
Cyberangriff (DDoS, Ransomware usw.)	WAF, Azure DDoS Protection und Sicherheitsüberwachung	Isolieren Sie kompromittierte Systeme und stellen Sie sie aus sauberen Backups wieder her

8 Null Vertrauen

8.1 Zero-Trust-Sicherheit verstehen

Vertrauen ist ein komplexes Konstrukt. Ich vertraue beispielsweise darauf, dass meine Mutter ein perfektes Abendessen kocht, aber ich würde ihr niemals die Netzwerksicherheit anvertrauen. In der Cybersicherheit kann falsches Vertrauen zu erheblichen Schwachstellen führen, weshalb es das Zero-Trust-Modell gibt.

8.1.1 Beispiel aus der Praxis: Die Gefahr impliziten Vertrauens

Einer der bekanntesten Sicherheitsverstöße, bei dem das Fehlen von Zero-Trust-Prinzipien eine Rolle spielte, war der **Angriff** auf **Colonial Pipeline** im Jahr 2021. Die Angreifer verschafften sich Zugang über kompromittierte VPN-Anmeldedaten, für die keine Multi-Faktor-Authentifizierung (MFA) aktiviert war. Da das Netzwerk authentifizierten Benutzern implizit vertraute, konnten sich die Angreifer lateral bewegen und Ransomware einsetzen, was zu einer weitreichenden Kraftstoffknappheit in den USA führte. Dieser Vorfall verdeutlicht, warum „niemals vertrauen, immer überprüfen“ für die moderne Cybersicherheit so wichtig ist.

8.2 Was ist Zero Trust?

Zero Trust ist ein Cybersicherheitsparadigma, das auf dem Prinzip „Niemals vertrauen, immer überprüfen“ basiert. Es stellt sicher, dass Benutzer und Geräte nicht standardmäßig vertraut werden, selbst wenn sie mit einem gesicherten Unternehmensnetzwerk verbunden sind oder zuvor überprüft wurden. Stattdessen muss das Vertrauen kontinuierlich anhand verschiedener Sicherheitssignale bewertet und validiert werden.

8.2.1 Die Grundprinzipien von Zero Trust

Zero Trust wird in **NIST SP 800-207** als ein Rahmenwerk definiert, das sich auf den Schutz von Ressourcen durch kontinuierliche Überprüfung konzentriert. Dieses Sicherheitsmodell gilt für:

- **Identitäts- und Zugriffsmanagement**: Sicherstellung einer sicheren Authentifizierung von Benutzern und Geräten.
- **Netzwerk- und Endpunktsicherheit**: Schutz der Kommunikation und Durchsetzung strenger Zugriffskontrollen.
- **Datenschutz**: Sicherstellen, dass sensible Daten verschlüsselt und sicher gespeichert werden.

- **Kontinuierliche Überwachung**: Erkennung von Anomalien und Reaktion auf potenzielle Bedrohungen in Echtzeit.

8.3 Wie Zero Trust auf MyQ Roger angewendet wird

8.3.1 Explizite Überprüfung

- Die Authentifizierung ist auch auf autorisierten Geräten (Smartphones/ Desktops) erforderlich.
- Verwendet moderne Authentifizierungsstandards.
- Für die Anmeldung bei Mobilgeräten und Multifunktionsdruckern (MFP) wird eine Multi-Faktor-Authentifizierung (MFA) vorgeschrieben.
- OAuth2 Device Flow wird für die Geräteautorisierung implementiert.
- **Kontinuierliche Authentifizierungsmechanismen** verfolgen Änderungen im Benutzerverhalten, um Anomalien zu erkennen.

8.3.2 Zugriffsverwaltung

- **Die rollenbasierte Zugriffskontrolle (RBAC)** stellt sicher, dass Benutzer nur über die minimal erforderlichen Zugriffsrechte verfügen.
- **Das Prinzip der geringsten Privilegien** wird angewendet, um Sicherheitsrisiken zu reduzieren.
- **Mikrosegmentierung** wird implementiert, um laterale Bewegungen innerhalb des Netzwerks zu begrenzen.
- **Just-in-Time-Zugriffskontrollen (JIT)** passen die Benutzerrechte dynamisch an den Kontext an.

8.3.3 Geräte- und Endpunktsicherheit

- Für jeden Gerätetyp werden eindeutige Zugriffstoken ausgegeben.
- Transport Layer Security (TLS) ist für die gesamte Kommunikation obligatorisch.
- **EDR-Lösungen (Endpoint Detection and Response)** überwachen und analysieren das Verhalten von Geräten.
- **Zero Trust Network Access (ZTNA)** stellt sicher, dass nur autorisierte Geräte auf bestimmte Ressourcen zugreifen können.

8.3.4 Datenschutz

- Alle Daten werden mithilfe verschlüsselter Speicherlösungen sicher gespeichert.
- Richtlinien stellen sicher, dass nur autorisierte Stellen auf die Daten zugreifen können.

- **Data Loss Prevention (DLP)-Lösungen** überwachen und verhindern unbefugte Datenexfiltration.
- **Sichere Enklaven** schützen hochsensible Daten vor unbefugtem Zugriff.

8.4 Bekämpfung von Cyber-Bedrohungen mit Zero Trust

Zero Trust hilft, die folgenden Bedrohungen zu mindern:

- **Insider-Bedrohungen**: Verhindert, dass Mitarbeiter oder kompromittierte Konten unbefugten Zugriff erhalten.
- **Credential Stuffing und Phishing-Angriffe**: Reduziert die Auswirkungen kompromittierter Anmeldedaten durch kontinuierliche Authentifizierung.
- **Lateral Movement-Angriffe**: Durch Mikrosegmentierung wird verhindert, dass Angreifer sich lateral über Netzwerke bewegen können.
- **Angriffe auf die Lieferkette**: Gewährleistet eine strenge Überprüfung des Zugriffs und der Integrationen von Drittanbietern.

8.5 Compliance- und regulatorische Überlegungen

Zero Trust entspricht verschiedenen Cybersicherheitsvorschriften und -rahmenwerken:

- **ISO 27001**: Erzwingt sicheres Zugriffsmanagement und Datenschutz.
- **DSGVO**: Gewährleistet die sichere Verarbeitung und Speicherung personenbezogener Daten.
- **HIPAA**: Schützt sensible Gesundheitsdaten.
- **NIST Cybersecurity Framework**: Bietet Richtlinien für die Implementierung von Zero Trust.

8.6 Warum Zero Trust wichtig ist

Die Einführung von Zero Trust minimiert das Risiko von Sicherheitsverletzungen, Insider-Bedrohungen und unbefugtem Zugriff. In einer Zeit zunehmender Cyber-Bedrohungen bietet eine Zero-Trust-Architektur robusten Schutz, indem sie eine kontinuierliche Überprüfung und strenge Zugriffskontrollen für alle Ressourcen gewährleistet.

Durch die Umsetzung dieser Prinzipien gewährleistet MyQ Roger eine sichere, widerstandsfähige und anpassungsfähige Sicherheitsstrategie, die den modernen Best Practices der Cybersicherheit entspricht. Darüber hinaus verbessern kontinuierliche Überwachung, Zugriffskontrollen und Echtzeit-Bedrohungserkennung die Fähigkeit des Unternehmens, effektiv auf sich entwickelnde Cyberbedrohungen zu reagieren.

9 Sicheres Login mit MyQ Roger

9.1 Einleitung

Die Verwendung einer PIN als primäre Anmeldemethode war nie wirklich sicher. Frühe Mobiltelefone basierten auf PINs, aber mit der Weiterentwicklung der Sicherheitsbedenken entwickelten sich auch die Authentifizierungsmethoden weiter. Heute sind biometrische Verfahren zur Norm geworden und bieten einen sichereren und benutzerfreundlicheren Ansatz für die Authentifizierung.

MyQ Roger hat sich dieser Entwicklung angeschlossen und die neueste OAuth 2.0 Device Authorization Grant (früher bekannt als Device Flow) implementiert. Bei dieser modernen Authentifizierungsmethode müssen sich Benutzer mit einem einmaligen QR-Code anmelden, der mit ihrem Mobiltelefon gescannt wird, sodass keine statischen Passwörter oder unsicheren PINs mehr erforderlich sind.

Wir betrachten das Mobiltelefon eines Benutzers als eines der sichersten Authentifizierungsmittel. Durch die Nutzung der biometrischen Authentifizierung zum Entsperren des Telefons und anschließenden Zugriff auf die MyQ-App stellen wir sicher, dass die sich anmeldende Person der rechtmäßige Eigentümer des Kontos ist.

9.2 Sichere Authentifizierung mit MyQ Roger

- **OAuth 2.0 Device Authorization Grant**: Anstelle von herkömmlichen PINs authentifizieren sich Benutzer mit einem dynamisch generierten QR-Code. Diese Methode reduziert das Risiko von Angriffen durch Diebstahl oder Wiederverwendung von Anmeldedaten erheblich.
- **Biometrische Verifizierung**: Da moderne Smartphones eine biometrische Verifizierung (z. B. Fingerabdruck oder Gesichtserkennung) zum Entsperren erfordern, wird dadurch eine zusätzliche Sicherheitsebene vor dem Zugriff auf MyQ Roger hinzugefügt.

9.3 Legacy-PIN-Authentifizierung

MyQ Roger bietet zwar weiterhin die Möglichkeit der PIN-basierten Anmeldung, diese Methode gilt jedoch als unsicher und wird standardmäßig nicht empfohlen. Benutzer, die sich für die PIN-Authentifizierung entscheiden, müssen diese ausdrücklich als sicher markieren und damit die damit verbundenen Sicherheitsrisiken anerkennen. Darüber hinaus werden durch die Aktivierung der PIN-

Anmeldung einige erweiterte Sicherheitsfunktionen deaktiviert, um potenzielle Schwachstellen zu minimieren.

9.4 Verantwortung für die Sicherheit

Wenn sich ein Unternehmen für die Zulassung der PIN-basierten Anmeldung entscheidet, liegt die Verantwortung für die Aufrechterhaltung einer sicheren Umgebung beim Kunden. Um Risiken zu minimieren, sollten bewährte Verfahren wie die Durchsetzung strenger PIN-Richtlinien, die Umsetzung physischer Sicherheitsmaßnahmen und die Überwachung von Zugriffsprotokollen befolgt werden.

9.5 Fazit

Mit MyQ Roger legen wir Wert auf Sicherheit, indem wir moderne Authentifizierungsstandards nutzen. Die Einführung der mobilen biometrischen Authentifizierung gewährleistet eine nahtlose und dennoch sichere Benutzererfahrung. Die herkömmliche PIN-basierte Anmeldung ist zwar weiterhin verfügbar, wird jedoch nicht empfohlen, und Kunden müssen zusätzliche Vorsichtsmaßnahmen treffen, wenn sie sich für diese Methode entscheiden. Durch die Einführung sicherer Anmeldemechanismen können Unternehmen sowohl die Sicherheit als auch die Benutzerfreundlichkeit für ihre Nutzer verbessern.

10 Sicheres Drucken mit MyQ Roger

10.1 Die Herausforderung des sicheren Druckens

Herkömmliche sichere Druckmethoden basieren auf physisch verbundenen Anschlüssen, wie z. B. LPT-Kabeln, bei denen ein dedizierter Drucker einem einzelnen Laptop zugewiesen ist. Diese Methode gewährleistet zwar ein Höchstmaß an Sicherheit, ist jedoch in modernen Umgebungen, die Flexibilität, Mobilität und gemeinsam genutzte Ressourcen erfordern, unpraktisch.

AirPrint und Mopria bieten zwar sichere Druckfunktionen, sind jedoch in Szenarien unzureichend, in denen Benutzer Remote-Druckaufträge auslösen können, ohne physisch in der Nähe des Druckers zu sein. Dies schafft Sicherheitslücken, da sensible Dokumente unbeaufsichtigt bleiben können.

10.2 MyQ Roger: Eine umfassende Lösung für sicheres Drucken

MyQ Roger integriert mehrere Druck-Workflows und setzt gleichzeitig Sicherheitsprotokolle durch, um sicherzustellen, dass Benutzer physisch anwesend sein müssen, um Druckaufträge zu authentifizieren und freizugeben. Das System garantiert, dass Druckaufträge sicher gespeichert und übertragen werden, während die Datenfreigabe minimiert wird.

10.3 Sichere Druckmethoden in MyQ Roger

10.3.1 1) Direktes Drucken vom PC zum Drucker

- Verwendet **IPP/s (Internet Printing Protocol Secure)** zur sicheren Übertragung von Druckaufträgen.
- Unterstützte Druckermarken: **Ricoh, Kyocera**.
- Druckaufträge bleiben direkt auf dem Drucker gespeichert, bis der Benutzer den Auftrag authentifiziert und freigibt.

10.3.2 2) MyQ Roger Client (MRC)

- Druckaufträge werden **verschlüsselt und lokal** auf dem PC des Benutzers **gespeichert**.
- Der Drucker ruft die verschlüsselte Datei **erst nach der Benutzerauthentifizierung** ab.
- Sicheres Drucken wird über **IPP/s** ausgeführt.

10.3.3 3) Cloud-Druck

- Druckdateien werden sicher im Cloud-Speicher des Benutzers (z. B. **OneDrive**, **Google Drive, Dropbox**) gespeichert.
- Der Drucker lädt das Dokument über einen **kurzlebigen Zugriffslink** direkt aus dem Cloud-Speicher herunter.
- Nach dem Drucken **werden keine Dokumente** auf dem Drucker **gespeichert**, wodurch die Vertraulichkeit der Daten gewährleistet ist.

10.3.4 4) Microsoft Universal Print Integration

- MyQ Roger implementiert einen **Universal Print Connector**, der es Druckern ermöglicht, direkt mit **den Universal Print-Servern von Microsoft** zu kommunizieren.
- Druckaufträge werden sicher auf **Microsoft-Servern** gespeichert und nach der Benutzerauthentifizierung bei Bedarf abgerufen.
- Der Druck erfolgt über **Universal Print-Treiber**, wodurch eine nahtlose und sichere Auftragsabwicklung gewährleistet ist.

10.4 Fazit

MyQ Roger bietet eine **ganzheitliche, sichere Druckumgebung**, indem es direkte, lokale und cloudbasierte Druck-Workflows mit robusten Sicherheitsmaßnahmen kombiniert. Da Benutzer sich vor der Ausführung eines Auftrags persönlich authentifizieren müssen, eliminiert MyQ Roger die mit unbeaufsichtigten Druckaufträgen verbundenen Risiken und gewährleistet maximalen Datenschutz in modernen Arbeitsumgebungen.

11 Geschäftskontakte

MyQ® Hersteller	**MyQ® GmbH** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prag 9, Tschechische Republik ID-Nr. 615 06 133 MyQ® spol. s r.o. ist im Handelsregister des Stadtgerichts in Prag unter der Nummer C 29842 eingetragen (im Folgenden als „MyQ®“ bezeichnet)
Geschäftsinformationen	http://www.myq-solution.com info@myq-solution.com[5]
Technischer Support	support@myq-solution.com[6]

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

Hinweis	DER HERSTELLER ÜBERNIMMT KEINE HAFTUNG FÜR VERLUSTE ODER SCHÄDEN, DIE DURCH DIE INSTALLATION ODER DEN BETRIEB DER SOFTWARE- UND HARDWARE-KOMPONENTEN DER MyQ®-DRUCKLÖSUNG ENTSTEHEN. Dieses Handbuch, sein Inhalt, sein Design und seine Struktur sind urheberrechtlich geschützt. Das Kopieren oder sonstige Vervielfältigen dieses Handbuchs oder von Teilen davon sowie aller urheberrechtlich geschützten Inhalte ohne vorherige schriftliche Zustimmung von MyQ® ist untersagt und kann strafbar sein. MyQ® übernimmt keine Verantwortung für den Inhalt dieses Handbuchs, insbesondere hinsichtlich seiner Vollständigkeit, Aktualität und kommerziellen Verwertbarkeit. Alle hier veröffentlichten Materialien dienen ausschließlich zu Informationszwecken. Dieses Handbuch kann ohne vorherige Ankündigung geändert werden. MyQ® ist nicht verpflichtet, diese Änderungen regelmäßig vorzunehmen oder anzukündigen, und ist nicht dafür verantwortlich, dass die derzeit veröffentlichten Informationen mit der neuesten Version der MyQ®-Drucklösung kompatibel sind.
Markenzeichen	„MyQ®“, einschließlich seiner Logos, ist eine eingetragene Marke von MyQ®. Jede Verwendung von Marken von MyQ®, einschließlich seiner Logos, ohne vorherige schriftliche Zustimmung der MyQ® Company ist untersagt. Die Marke und der Produktname sind durch MyQ® und/oder seine lokalen Tochtergesellschaften geschützt.

myQ roger

SPAREN SIE ZEIT MIT PERSONALISIERTEN DRUCKLÖSUNGEN

MyQ Roger ist eine Lösung für moderne, cloudbasierte Arbeitsumgebungen. Sie vereinfacht Dokumenten-Workflows und ermöglicht das sichere Durchsuchen von CloudSpeichern sowie Drucken und Scannen – jederzeit und überall.

info@myq-solution.com

myq-solution.com

50+ Millionen
Nutzer weltweit vertrauen auf MyQ

1+ Million
Aktive Geräte

26+
Unterstützte Hersteller

1000+
Zertifizierte Partner

Im Einsatz in über
140 Ländern

Ausgezeichnet und zertifiziert

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001