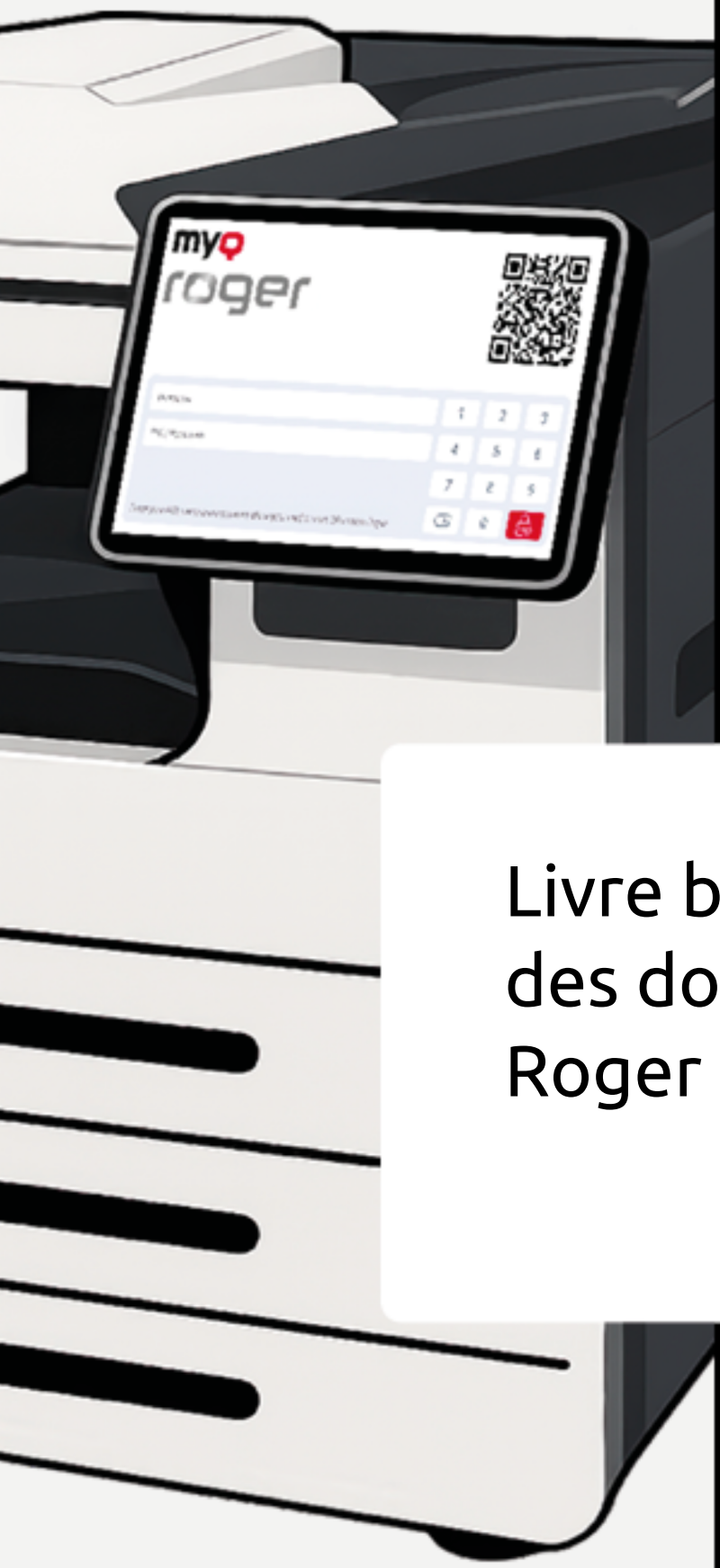

Livre blanc sur la sécurité des données de MyQ Roger 2.x

Généré à partir de docs.myq-solution.com
août/2026

FRANÇAIS

Avis sur la traduction

Cette traduction a été réalisée avec l'aide de l'intelligence artificielle. En cas de divergence ou d'ambiguïté, le document source en anglais fait foi.

Table des matières

1 Introduction

Le présent document a pour objectif d'informer les clients de MyQ Roger des processus impliquant l'établissement de connexions dans le système et des mesures de sécurité prises pour protéger le transfert de données qui en résulte.

Les thèmes suivants sont abordés :

- Glossaire : résumé de la terminologie utilisée.
- Sécurité des opérations : examen approfondi des systèmes de surveillance, de l'infrastructure et des workflows de développement afin de garantir la sécurité de MyQ Roger.
- Sécurité des applications : décrit l'approche de MyQ Roger en matière de sécurité, en détaillant les responsabilités des différentes parties, l'automatisation et la gestion.
- Protection des données : résume les normes de MyQ Roger en matière de sécurité cloud multi-locataires, de cryptage et de communication sécurisée, ainsi que de conformité et de gestion des identités. Contient également des dispositions relatives à la conformité au RGPD et à la sauvegarde des données.
- Disponibilité des serveurs, sauvegarde des données et reprise après sinistre : détaille la surveillance de l'état fournie par MyQ Roger et les stratégies de sauvegarde et les plans d'intervention disponibles.
- Zero Trust : examine la signification et l'importance de la sécurité Zero Trust et décrit comment MyQ Roger se conforme à ces principes.
- Connexion sécurisée avec MyQ Roger : détaille les mesures prises par MyQ Roger pour garantir la sécurité de la connexion.
- Impression sécurisée avec MyQ Roger : fournit des détails sur les différentes méthodes d'impression utilisées par MyQ Roger et les mesures de sécurité qui accompagnent chacune d'entre elles.

2 Guide PDF

Ce guide est également disponible au format PDF.

File	Size
MyQ Roger Data Security Whitepaper.pdf	3.2 MB

3 Glossaire

- **IPP/s (Internet Printing Protocol over Secure TLS)** :
  - MyQ Roger garantit une impression sécurisée en utilisant le protocole d'impression Internet (IPP) sur un canal crypté TLS, empêchant ainsi tout accès non autorisé et garantissant l'intégrité des données en transit.
  - MyQ Roger optimise le trafic réseau grâce à une gestion efficace des paquets, réduisant ainsi les transmissions de données inutiles et garantissant une communication sécurisée entre les points d'extrémité.
- **TLS (Transport Layer Security)** :
  MyQ Roger applique le protocole TLS 1.2/1.3 pour un cryptage sécurisé des données dans toutes les communications, garantissant une protection contre les interceptions et les attaques de type « man-in-the-middle » (MITM).
- **Données au repos, données en transit** :
  - **Données au repos** : MyQ Roger crypte les données stockées à l'aide de l'algorithme AES-256, garantissant ainsi la sécurité des informations sensibles contre tout accès non autorisé.
  - **Données en transit** : toutes les données transférées entre les clients, les serveurs et les services cloud sont cryptées à l'aide du protocole TLS afin de garantir leur intégrité et leur confidentialité.
- **Infrastructure Zero Trust** :
  MyQ Roger suit un modèle de sécurité **Zero Trust** en mettant en œuvre une authentification continue, une vérification des périphériques et un accès avec privilèges minimaux pour les utilisateurs et les services.
- **IAM (gestion des identités et des accès)** :
  MyQ Roger intègre les meilleures pratiques IAM en appliquant une authentification sécurisée des utilisateurs, une authentification multifactorielle (MFA) et des contrôles d'accès basés sur l'identité.
- **RBAC (contrôle d'accès basé sur les rôles)** :
  MyQ Roger met en œuvre le RBAC pour restreindre les autorisations en fonction des rôles des utilisateurs, garantissant ainsi que seul le personnel autorisé peut accéder aux fonctions critiques et aux données sensibles.
- **SSO (authentification unique)** :
  MyQ Roger prend en charge **le SSO** via l'intégration OAuth2, ce qui permet une authentification transparente dans toutes les applications d'entreprise tout en garantissant la sécurité et la conformité.

4 Sécurité des opérations

4.1 Introduction

La sécurité est une priorité absolue chez MyQ Roger. Nous appliquons une approche **axée sur la sécurité** à chaque étape du développement, du déploiement et des opérations. Compte tenu de la nature critique des environnements cloud, la sécurité doit être **proactive, automatisée et surveillée en permanence** afin de prévenir les violations et les accès non autorisés.

Notre **stratégie d'opérations sécurisées** intègre **une surveillance continue, la gestion des vulnérabilités, la sécurité des infrastructures et la conformité** afin de garantir l'intégrité des applications et des infrastructures.

4.2 Surveillance

La surveillance continue est essentielle pour détecter et répondre aux menaces en temps réel. MyQ met en œuvre une **approche de surveillance à plusieurs niveaux :**

4.2.1 Détection et réponse aux incidents au niveau des terminaux (EDR)

- Surveille tous les terminaux (serveurs, machines virtuelles et conteneurs) à la recherche d'activités suspectes.
- Utilise **l'analyse comportementale et les renseignements sur les menaces** pour détecter les menaces avancées.
- Isole automatiquement les terminaux compromis pour empêcher tout mouvement latéral.

4.2.2 Azure Defender (désormais Defender for Cloud)

- Protège **Azure AKS, SQL Server, les machines virtuelles et le stockage**.
- Fournit **une détection des menaces en temps réel** et des recommandations de configuration de sécurité.
- S'intègre à **Microsoft Sentinel (SIEM)** pour une alerte centralisée.

4.2.3 Analyse des hôtes

- Analyse **les machines virtuelles, les instances cloud et les serveurs sur site** à la recherche de configurations incorrectes et de logiciels obsolètes.
- Détecte **les risques d'escalade de privilèges, les points d'accès non autorisés et les dépendances obsolètes.**

4.2.4 Collecte et analyse des journaux

- **Journalisation centralisée** sur un cluster séparé pour plus d'évolutivité et d'isolation.
- **Les journaux provenant de Kubernetes, des applications et de l'infrastructure** sont étiquetés pour une récupération efficace.
- **Les politiques de conservation à long terme** garantissent la conformité et l'analyse de la sécurité.
- **Les mécanismes d'alerte** détectent les anomalies et les incidents de sécurité, en s'intégrant au SIEM.
- **Corrélation des journaux en temps réel** pour les requêtes API, les événements d'authentification, les requêtes de base de données et le trafic du pare-feu.

4.2.5 Analyse des ports

- Détecte **les ports ouverts** non autorisés qui exposent les services à des menaces.
- Utilise **des outils automatisés tels que Nmap et ZMap** pour rechercher **les changements de ports inattendus**.

4.2.6 Analyse des conteneurs

- **Analyse statique et dynamique** des conteneurs Docker avant leur déploiement.
- Identifie les vulnérabilités dans **les images de base, les couches d'application et les autorisations d'exécution**.
- Intégration avec **Trivy** pour **l'analyse de sécurité des images**.

4.2.7 Surveillance Kubernetes

- Utilise **la surveillance embarquée Azure Kubernetes Service (AKS)** avec **Prometheus & Grafana**.
- Surveille **les appels API Kubernetes, les politiques RBAC et la sécurité des pods**.
- Alerte en cas **d'escalade des privilèges des conteneurs, d'utilisation excessive des ressources et de tentatives de mouvement latéral**.

4.2.8 Analyses TLS régulières

- MyQ effectue **des analyses de sécurité TLS à l'aide de Qualys SSL Labs** afin de garantir le respect des meilleures pratiques.
- Les configurations TLS sont évaluées afin de maintenir une **note de sécurité A+**, ce qui permet d'atténuer les risques liés aux protocoles faibles.

- Des outils automatisés vérifient **la validité des certificats, le suivi des expirations et la force des protocoles**.

4.3 Gestion des vulnérabilités

4.3.1 Analyse des vulnérabilités

- **Des analyses régulières** détectent les failles de sécurité dans les applications et l'infrastructure.
- Comprend **l'analyse CVE automatisée** pour les composants déployés dans le cloud.
- S'intègre à **DefectDojo, SonarQube et Trivy** pour l'évaluation des risques.

4.3.2 Tests de pénétration

- Réalisés régulièrement pour identifier les failles de sécurité avant qu'elles ne soient exploitées.
- Combine **des méthodologies de test automatisées et manuelles** pour une évaluation complète.
- Les résultats sont **documentés, classés par ordre de priorité et corrigés** en conséquence.

4.4 Sécurité de l'infrastructure

Une **infrastructure renforcée** garantit une sécurité qui va au-delà de la simple surveillance. MyQ utilise :

4.4.1 SIEM (gestion des informations et des événements de sécurité)

- **Microsoft Sentinel SIEM** collecte les événements de sécurité pour une détection en temps réel.
- Analyse les journaux des **pare-feu, des systèmes d'identité, des applications, des audits et des flux de menaces**.
- Permet **des réponses automatisées aux menaces détectées**.

4.4.2 Suivi et gestion de la sécurité

- **La base de données Jira Bug** suit, classe et hiérarchise les vulnérabilités de sécurité.
- **DefectDojo** consolide les résultats des tests, garantissant un suivi structuré des engagements en matière de sécurité.
- **Des correctifs et des remèdes** réguliers permettent de maintenir une posture de sécurité solide.

4.4.3 Gestion des identités et des accès (IAM)

- Applique **le principe du « zéro confiance »** grâce **au contrôle d'accès basé sur les rôles (RBAC) et à l'authentification multifactorielle (MFA)**.
- Utilise **Azure AD** pour la gouvernance des identités.
- **Les alertes d'escalade de privilèges** détectent les accès administrateur non autorisés.

4.5 Workflow de développement

Le développement sécurisé de logiciels est un aspect essentiel de la stratégie de sécurité de MyQ. Les mesures suivantes garantissent l'intégrité du code, des pipelines et des environnements cloud :

4.5.1 Environnement de développement sécurisé

- Les développeurs MyQ utilisent **des environnements sécurisés** avec protection des terminaux.
- Les développeurs doivent suivre **des pratiques de codage sécurisées et suivre régulièrement des formations sur la sécurité**.

4.5.2 Pipelines sécurisés GitLab

- Les pipelines GitLab CI/CD comprennent **des contrôles de sécurité automatisés, des revues de code et des tests**.
- **Les tests de sécurité statiques des applications (SAST)** et **les tests de sécurité dynamiques des applications (DAST)** détectent les vulnérabilités.
- **La signature des images de conteneurs** garantit que seules les images fiables sont déployées.

4.5.3 IAM et contrôle d'accès

- Seuls **les membres sélectionnés des équipes DevOps et SecOps** ont accès aux environnements cloud Azure.
- **Un contrôle d'accès basé sur les rôles (RBAC) avec élévation des privilèges minimaux juste à temps (JIT)** est appliqué.

4.5.4 Sécurité Azure Kubernetes et des conteneurs

- **Les clusters AKS** de MyQ **extraient les images uniquement à partir du registre de conteneurs Azure (ACR)**.
- Les environnements AKS appliquent **des politiques réseau et des normes de sécurité des pods (PSS)** afin d'isoler les charges de travail.

4.5.5 Gestion des secrets

- **Tous les secrets et clés API sont stockés dans Azure Key Vault**, accessible uniquement au personnel autorisé par IAM.
- **Des analyses du système de fichiers Trivy** sont effectuées avant la validation dans Git afin de détecter et d'empêcher les secrets sensibles.

4.6 Conclusion

La stratégie de sécurité des opérations de MyQ repose sur une **surveillance continue, une gestion proactive des menaces et une sécurité solide de l'infrastructure**. En tirant parti **d'outils de sécurité avancés, de contrôles d'accès stricts et de tests automatisés**, MyQ garantit un **environnement cloud sécurisé et résilient**.

Grâce à l'**intégration de scans de sécurité TLS, de tests de pénétration et d'une journalisation centralisée**, MyQ renforce sa capacité à **détecter, répondre et atténuer** efficacement **les risques de sécurité**.

La sécurité est un **défi en constante évolution**, et MyQ reste déterminé à **renforcer ses mesures de sécurité par des mises à jour régulières, des audits de conformité et des bonnes pratiques en matière de sécurité**. En privilégiant la **sécurité**, MyQ préserve l'**intégrité et la confidentialité** de ses services, garantissant **ainsi la confiance et la fiabilité** de toutes les parties prenantes.

5 Sécurité des applications

5.1 L'évolution des menaces pour la sécurité

À l'époque où Internet n'était pas encore très répandu, les imprimantes étaient directement connectées via des câbles LPT et les problèmes de sécurité étaient minimes. Le plus grand risque était physique : quelqu'un pouvait regarder par-dessus l'épaule d'un utilisateur pour voir les documents imprimés. Le paysage de la sécurité était simple et les cybermenaces pratiquement inexistantes.

Cependant, avec la connexion des imprimantes et des périphériques au réseau, le paysage des menaces a radicalement changé. Les imprimantes étant désormais accessibles via les réseaux locaux (LAN) et même Internet, les pirates n'ont plus besoin d'un accès physique. Les menaces telles que les attaques de type « man-in-the-middle » (MITM), l'interception non autorisée de données et les exploits à distance sont devenues courantes. Les cybercriminels sont passés de l'espionnage à l'écoute du trafic réseau et à l'exploitation des vulnérabilités.

Atténuer ces risques est un défi permanent, car de nouvelles menaces apparaissent fréquemment. Pour relever ces défis de sécurité en constante évolution, MyQ Roger met en œuvre des pratiques de sécurité continues, une surveillance proactive et des mécanismes de défense solides.

5.2 L'approche de MyQ Roger en matière de sécurité

MyQ Roger est conçu selon une approche axée sur la sécurité, garantissant que l'innovation et l'expérience utilisateur sont toujours conformes aux normes de sécurité les plus strictes. Notre engagement en matière de sécurité se reflète dans nos efforts continus pour intégrer des mesures de sécurité robustes à chaque étape du développement. Nous adoptons une philosophie de « sécurité par défaut », en intégrant la sécurité dans nos produits et services dès leur conception.

Pour y parvenir, MyQ Roger s'appuie sur l'automatisation, l'évaluation des risques basée sur les données et les meilleures pratiques de sécurité pour identifier et atténuer de manière proactive les menaces. En mettant en œuvre des contrôles de sécurité dès le début du cycle de développement, selon une **approche « shift left »**, nous nous assurons que les vulnérabilités sont détectées et corrigées avant qu'elles n'atteignent la phase de production. Cette intégration proactive nous permet d'évoluer efficacement, de réduire les risques et de minimiser les menaces de

sécurité. Notre approche renforce notre engagement à protéger les données des clients, les flux de travail et la sécurité globale.

5.3 Shifting Left en matière de sécurité

Le « shift left » en matière de sécurité consiste à intégrer la sécurité dès le début du cycle de vie du développement logiciel (SDLC) plutôt que de traiter les vulnérabilités plus tard. En détectant les problèmes de sécurité dès les premières étapes du développement, nous évitons des corrections coûteuses et atténuons les violations potentielles. Cette stratégie proactive garantit que chaque ligne de code répond aux normes de sécurité les plus élevées avant d'atteindre la phase de production, ce qui réduit les risques et renforce notre posture de sécurité globale.

5.4 Responsabilités de MyQ en matière de sécurité

MyQ Roger s'engage à protéger les données des clients et à garantir un environnement opérationnel sécurisé. Nos principales responsabilités en matière de sécurité sont les suivantes :

- **Protection des données** : MyQ veille à ce que les données des clients soient stockées et cryptées de manière sécurisée, empêchant tout accès non autorisé et garantissant la confidentialité des données.
- **Correctifs de sécurité réguliers** : nous appliquons de manière proactive des correctifs et des mises à jour de sécurité à tous les systèmes afin d'éliminer les vulnérabilités avant qu'elles ne puissent être exploitées.
- **Gestion du contrôle d'accès** : nous appliquons des politiques d'accès strictes suivant le principe du moindre privilège, garantissant que seul le personnel autorisé peut accéder aux ressources sensibles.

En respectant ces principes de sécurité, MyQ Roger favorise une culture de la sécurité, protégeant les utilisateurs contre les menaces potentielles tout en garantissant la conformité aux normes industrielles.

5.5 Contrôle/gestion de la sécurité MyQ Roger

Bien que nous nous appuyions sur une infrastructure cloud sécurisée, MyQ Roger assume la responsabilité directe de la mise en œuvre de couches de sécurité supplémentaires et du respect des meilleures pratiques du secteur. Notre approche comprend :

- **Gestion des clés avec Azure Key Vault** : nous utilisons Azure Key Vault pour stocker et gérer de manière sécurisée tous les secrets, clés privées et certificats, en garantissant des contrôles d'accès et un cryptage stricts.

- **Certification ISO 27001** : nous adhérons aux normes ISO 27001 afin de maintenir une approche structurée et cohérente en matière de sécurité de l'information.
- **Détection et réponse aux incidents au niveau des terminaux (EDR)** : nous exploitons des solutions EDR avancées pour détecter, analyser et atténuer les menaces de sécurité en temps réel, réduisant ainsi le temps de réponse et minimisant les risques.
- **Pratiques de développement sécurisées** : notre cycle de vie de développement logiciel sécurisé comprend des évaluations de vulnérabilité, une surveillance continue et des analyses de sécurité automatisées pour détecter et corriger les failles de sécurité.
- **Audits de sécurité réguliers** : nous effectuons des audits internes et externes afin de garantir la conformité et de traiter de manière proactive les risques de sécurité.
- **SIEM avec Azure Sentinel** : nous utilisons Azure Sentinel pour la détection des menaces en temps réel, la réponse automatisée et la surveillance continue de la sécurité dans tous les environnements cloud et réseau.

En mettant en œuvre ces mesures de sécurité, MyQ Roger renforce son cadre de sécurité global, garantissant ainsi la protection des données des clients à tout moment.

5.6 Microsoft Azure et conformité

MyQ Roger fonctionne sur Microsoft Azure, en tirant parti des services Azure Kubernetes Service (AKS), Azure SQL Servers et Azure Cosmos DB pour MongoDB. En opérant au sein de l'infrastructure Azure, nous bénéficions des normes de sécurité, de conformité et de fiabilité de pointe de Microsoft.

5.6.1 Responsabilités de Microsoft en matière de sécurité et de conformité

- Azure adhère à des cadres de conformité mondiaux tels que ISO 27001, SOC 2 et GDPR dans l'UE, garantissant le respect de normes réglementaires strictes.
- Microsoft fournit des fonctionnalités de sécurité embarquées telles que l'isolation du réseau, la protection de l'identité et la détection continue des menaces, réduisant ainsi les surfaces d'attaque.
- Les services Azure sont soumis à des évaluations de sécurité et à des tests de pénétration rigoureux afin d'identifier et de corriger de manière proactive les vulnérabilités.

En tirant parti de l'infrastructure sécurisée d'Azure, MyQ Roger ajoute ses propres couches de sécurité pour créer un modèle de sécurité robuste et résilient qui protège les applications et les données des clients.

5.7 Responsabilités des clients en matière de sécurité

Bien que MyQ Roger fournisse une infrastructure sécurisée et des mesures de sécurité de premier ordre, les clients ont également des responsabilités clés pour garantir la sécurité de leur environnement. Il s'agit notamment de :

- **Tenir à jour une liste d'utilisateurs actifs** : les clients doivent gérer en permanence l'accès des utilisateurs en tirant parti de la synchronisation automatisée des utilisateurs ou en désactivant manuellement les comptes inactifs afin de minimiser les risques.
- **Application du contrôle d'accès basé sur les rôles (RBAC)** : les clients doivent appliquer les principes du RBAC pour limiter l'accès des utilisateurs aux seules autorisations nécessaires, garantissant ainsi une sécurité et une efficacité opérationnelle accrues.
- **Sécurisation du réseau local** : même si MyQ Roger fonctionne selon un modèle « zero trust », les clients doivent s'assurer que leur réseau local respecte les meilleures pratiques en matière de sécurité, telles que la configuration de pare-feu, la segmentation du réseau et la protection des terminaux.
- **Maintenance adéquate des ressources** : tous les périphériques connectés, y compris les imprimantes et les appareils multifonctions (MFP), doivent être régulièrement mis à jour avec les derniers micrologiciels et correctifs de sécurité afin de prévenir les vulnérabilités.

En respectant ces responsabilités, les clients renforcent leur posture de sécurité tout en bénéficiant du cadre de sécurité complet de MyQ Roger.

5.8 Automatisation de la sécurité

Afin de renforcer encore la sécurité tout au long du cycle de développement, MyQ Roger intègre des tests de sécurité automatisés et des évaluations de sécurité externes :

- **SAST (tests statiques de sécurité des applications)** : effectués à chaque validation afin de détecter les vulnérabilités de sécurité dès le début du cycle de développement, réduisant ainsi le risque que du code non sécurisé atteigne la production.
- **DAST (tests de sécurité dynamiques des applications)** : effectués dans des environnements sandbox afin d'identifier et d'atténuer les risques de sécurité d'exécution avant le déploiement.

- **Tests de pénétration externes** : nous faisons appel à des experts en sécurité indépendants pour effectuer des tests de pénétration, afin de nous assurer que nos défenses de sécurité peuvent résister à des scénarios d'attaque réels.

En automatisant les tests de sécurité et en effectuant régulièrement des évaluations externes, MyQ Roger maintient une posture de sécurité proactive et résiliente.

5.9 Conclusion

Chez MyQ Roger, la sécurité n'est pas une réflexion après coup, elle fait partie intégrante de notre produit et de notre cycle de développement. En combinant les principes de sécurité dès la conception, les meilleures pratiques du secteur et un cadre de conformité solide, nous offrons une posture de sécurité robuste qui protège les données et les opérations de nos clients. Notre engagement en faveur d'améliorations continues en matière de sécurité garantit que MyQ Roger reste résilient face à l'évolution des menaces tout en maintenant les normes les plus élevées de fiabilité et de confiance. Nous continuerons à faire évoluer notre stratégie de sécurité, en nous adaptant aux nouveaux défis et en tirant parti des dernières technologies afin de respecter notre mission qui consiste à offrir une expérience utilisateur sécurisée et fluide.

6 Protection des données

6.1 Présentation

La protection des données est au cœur de l'approche **de MyQ Roger** en matière de sécurité, garantissant que chaque aspect de sa solution d'impression et de numérisation basée sur le cloud respecte les normes les plus strictes du secteur. L'un des principes fondamentaux de MyQ Roger est qu'**aucune donnée relative aux travaux d'impression ou de numérisation n'est jamais transférée via ses serveurs**. Au lieu de cela, MyQ Roger limite strictement sa collecte de données aux **métadonnées** essentielles, telles que **les noms de fichiers, la taille des fichiers et le nombre de pages**. Cela garantit l'efficacité opérationnelle tout en protégeant la vie privée des utilisateurs.

6.2 Sécurité cloud multi-locataires

En tant que **produit cloud multi-locataires**, MyQ Roger offre à ses clients un environnement **logiquement isolé** afin d'empêcher l'exposition des données entre locataires.

Pour garantir sa résilience, MyQ Roger s'appuie sur **Azure SQL** et **Azure Cosmos DB**, qui offrent tous deux des fonctionnalités de sécurité embarquées telles que **le chiffrement des données au repos et en transit, la détection automatisée des menaces et la surveillance des accès**. L'infrastructure cloud fait l'objet d'évaluations de sécurité continues afin d'atténuer les risques associés aux environnements multi-locataires.

6.3 Chiffrement et communication sécurisée

La sécurité est intégrée à tous les niveaux des opérations de MyQ Roger. Toutes les communications entre les clients, les services cloud et les imprimantes sont **cryptées à l'aide du protocole TLS (Transport Layer Security)** afin d'empêcher tout accès non autorisé ou toute altération.

Pour renforcer encore la sécurité, **des autorités de certification (CA) reconnues** signent tous les certificats utilisés dans MyQ Roger, garantissant ainsi le plus haut niveau de confiance. De plus, les certificats sont **renouvelés tous les trois mois**, ce qui réduit le risque de compromission potentielle et garantit le respect des meilleures pratiques en matière de sécurité.

6.4 Conformité et gestion des identités

MyQ Roger se conforme aux normes de sécurité internationalement reconnues et détient **la certification ISO 27001**, qui démontre son engagement à mettre en œuvre des pratiques rigoureuses en matière de gestion de la sécurité de l'information.

Afin d'appliquer des contrôles d'accès stricts, **un contrôle d'accès basé sur les rôles (RBAC)** est mis en œuvre, garantissant que les utilisateurs **ne** se voient accorder **que les autorisations nécessaires à leur rôle**. Cela minimise l'exposition aux données sensibles et réduit le risque d'utilisation abusive accidentelle ou intentionnelle.

6.5 Conformité au RGPD

La conformité au **règlement général sur la protection des données (RGPD)** est une priorité absolue pour MyQ Roger. Conformément aux principes du RGPD, MyQ Roger applique des mesures strictes de protection des données afin de préserver la confidentialité des utilisateurs :

- **Minimisation des données** : seules les métadonnées essentielles sont collectées, ce qui élimine le risque de stockage de documents sensibles des utilisateurs.
- **Droits et contrôle des utilisateurs** : les utilisateurs ont la possibilité de demander **l'accès, la correction, la suppression ou l'anonymisation** de leurs données personnelles, comme l'exige le RGPD.
- **Transparence dans le traitement des données** : des politiques de confidentialité claires et concises décrivent la manière dont les métadonnées sont traitées, stockées et protégées.
- **Stockage sécurisé des données** : toutes les données sont **cryptées au repos et en transit**, garantissant ainsi le respect total des exigences strictes du RGPD en matière de sécurité.
- **Mesures d'anonymisation** : lorsque cela est nécessaire, MyQ Roger met en œuvre **des techniques d'anonymisation des données** afin de garantir que les données personnelles ne puissent plus être attribuées à un utilisateur spécifique, renforçant ainsi la protection de la vie privée.

Ces mesures garantissent que MyQ Roger se conforme pleinement aux exigences fondamentales du RGPD, en donnant aux utilisateurs le contrôle de leurs données personnelles tout en maintenant un environnement sécurisé et conforme.

6.6 Sauvegardes de données

Afin de se prémunir contre la perte de données et de garantir la fiabilité du service, MyQ Roger met en œuvre une **stratégie complète de sauvegarde des données**. Celle-ci comprend :

- **Sauvegardes automatisées** : **des sauvegardes incrémentielles et complètes** régulières garantissent que les données restent récupérables en cas d'incident.
- **Stockage sécurisé** : les sauvegardes sont cryptées à l'aide **du cryptage AES-256**, garantissant que même dans le cas improbable d'un accès non autorisé, les données restent illisibles.
- **Politiques de conservation** : les sauvegardes sont **conservées pendant une période définie**, conformément aux exigences de conformité, ce qui permet une récupération efficace en cas de panne du système ou de scénario de reprise après sinistre.
- **Tests et vérification de l'intégrité** : **des tests d'intégrité des sauvegardes** sont effectués régulièrement afin de confirmer que les sauvegardes stockées sont fonctionnelles et fiables, garantissant ainsi une restauration transparente des données en cas de besoin.

Grâce à la mise en œuvre de ces mesures robustes en matière de sécurité, de conformité et de sauvegarde, **MyQ Roger fournit une solution d'impression et de numérisation basée sur le cloud sécurisée, privée et hautement efficace,** qui répond aux normes de protection des données les plus strictes du secteur.

7 Politique de confidentialité

Nous prenons votre vie privée très au sérieux. La présente politique de confidentialité de MyQ Roger Solution (la « politique de confidentialité ») explique le type d'informations que MyQ peut collecter, conserver et traiter dans le cadre de la fourniture de tout produit, service, contenu, application ou autre composant faisant partie de MyQ Roger Solution (les « services »), ainsi que la manière dont ces informations sont utilisées et protégées. Elle indique également comment vous pouvez nous contacter si vous avez des questions ou des préoccupations concernant vos données personnelles.

La présente Politique de confidentialité est publiée par MyQ, spol. s.r.o., dont le siège social est situé à Českomoravská 2420/15, Libeň, 190 00 Praha 9, République tchèque, numéro d'identification de la société 615 06 133, inscrite au registre du commerce tenu par le tribunal municipal de Prague, section C, insert 29842 (« MyQ » ou « nous »).

Nous nous réservons le droit de modifier la présente politique de confidentialité à tout moment. Veuillez consulter régulièrement la politique de confidentialité pour prendre connaissance des modifications, mais si vous êtes client, nous pouvons également vous informer par e-mail de toute modification qui, à notre seule discrétion, a une incidence significative sur votre utilisation des services ou sur la manière dont nous traitons vos données personnelles. En continuant à utiliser nos services couverts par la présente politique de confidentialité, vous acceptez toutes les modifications que nous apportons de temps à autre à la présente politique de confidentialité.

7.1 1. Données que nous collectons ou recevons

Nous collectons des données personnelles auprès de nos clients, en tant qu'utilisateurs des Services, et de leurs utilisateurs finaux (qui comprennent les employés de nos clients) afin de créer et de gérer des comptes d'utilisateurs et de fournir et d'administrer les Services. Nous collectons également des données et des mesures d'utilisation. Nous sommes le responsable du traitement de ces données personnelles.

En ce qui concerne les données personnelles qui peuvent être incluses dans les métadonnées du Contenu, telles que définies dans les Conditions d'utilisation https://www.myq-solution.com/en/myq-legal-documents , que les utilisateurs ou les utilisateurs finaux gèrent à l'aide des Services, ou en ce qui concerne les données

personnelles auxquelles nous pouvons avoir accès lorsque nous fournissons des services d'assistance à distance ou sur site (les « Données client »), nous traitons ces données personnelles pour le compte de nos clients en tant que sous-traitant. Lorsque nous traitons les Données client afin de fournir les Services à nos clients, nous agissons conformément aux instructions de nos clients en tant que sous-traitant. Nous conservons toujours les Données client que nous traitons pour le compte de nos clients et conformément à leurs instructions séparément des données de nos autres clients et les gardons strictement confidentielles.

7.1.1 1.1 Données des utilisateurs et des utilisateurs finaux de nos Services

Nous collectons vos données personnelles lorsque :

- Vous créez un compte au sein de nos Services ;
- Vous vous connectez à notre Service en saisissant votre nom d'utilisateur (adresse e-mail) et votre mot de passe ;
- Vous utilisez nos Services ou interagissez de toute autre manière avec MyQ, par exemple lorsque vous nous soumettez des questions ;
- Vous fournissez volontairement ces données à MyQ.

Lorsque vous créez un compte auprès de MyQ, nous vous demandons de remplir un formulaire d'inscription en indiquant votre prénom, votre nom, votre adresse e-mail, votre entreprise et votre fonction. Vous pouvez également choisir d'ajouter un numéro de téléphone à votre compte.

Nous collectons et traitons également votre nom d'utilisateur (adresse e-mail) et votre mot de passe.

À des fins d'analyse et d'amélioration de nos Services, nos serveurs peuvent enregistrer automatiquement des informations lorsque vous visitez notre site web ou utilisez certains de nos Services (« données d'utilisation »), notamment :

- Informations sur les services tiers auxquels l'utilisateur et ses utilisateurs finaux se connectent aux Services à des fins d'authentification et de connexion au stockage cloud de l'utilisateur ;
- des informations sur les périphériques de l'utilisateur, par exemple le type et la marque des imprimantes et leur numéro de série ;
- des informations sur l'utilisation de nos Services, par exemple le nombre de documents imprimés ou numérisés.

Les Services vous permettent de vous connecter à des applications tierces ou à d'autres services, par exemple One Drive ou Google Disk, dans le but de partager des documents et d'autres contenus avec les Services. Si vous choisissez de vous

connecter à des services tiers, nous vous demanderons votre autorisation pour permettre aux Services d'accéder à ces services tiers. Cependant, MyQ ne traitera aucune donnée personnelle stockée sur ces services, à l'exception des Données client, telles que définies ci-dessus.

Si nos Services sont achetés par une entité, ce sont les utilisateurs individuels au sein de l'organisation de cette entité qui se connectent à notre plateforme de Services et dont les données personnelles sont collectées, comme décrit ci-dessus. Lorsque cette entité nous fournit directement les données personnelles de ses employés ou d'autres utilisateurs individuels qu'elle a autorisés à accéder aux Services, elle doit disposer de tous les consentements, autorisations ou enregistrements nécessaires pour traiter et nous fournir les données personnelles de ses employés ou utilisateurs.

7.1.2 1.2 Données client

Afin de fournir nos Services à nos utilisateurs et utilisateurs finaux, nous pouvons également traiter les Données client, telles que définies ci-dessus. Le traitement des Données client est soumis à la politique de confidentialité des utilisateurs, et ces derniers sont tenus de s'assurer que le traitement de ces données est légal et conforme à la législation applicable. Le traitement des Données client effectué par MyQ est régi par les accords de traitement des données applicables conclus avec les utilisateurs.

7.2 2. Comment nous utilisons les données

Nous utilisons vos données personnelles aux fins suivantes :

7.2.1 2.1 Pour fournir les Services

Nous pouvons traiter vos données personnelles afin de vous identifier lorsque vous vous connectez à votre compte et utilisez nos Services, afin de nous permettre d'exploiter les Services et de vous les fournir. Cela peut inclure la vérification de vos paiements, de vos bons de commande et de vos informations de facturation.

7.2.2 2.2 Pour communiquer avec vous

Nous pouvons traiter les données de nos clients ou de leurs utilisateurs finaux individuels, en particulier les adresses e-mail ou autres coordonnées, afin de communiquer avec nos utilisateurs et utilisateurs finaux, par exemple lorsque nous les aidons à configurer ou à gérer leur compte, lorsque nous fournissons un service client et une assistance, envoyons des avis techniques, des mises à jour concernant

les changements ou améliorations à venir des Services, des rappels, des alertes de sécurité et d'autres messages d'assistance et administratifs.

7.2.3 2.3 Pour offrir une meilleure expérience utilisateur

Nous pouvons traiter vos données personnelles afin de comprendre comment vous utilisez nos Services et ainsi améliorer continuellement l'expérience utilisateur et fournir un service client fluide. Nous pouvons également traiter ces données personnelles afin d'améliorer et de renforcer nos Services existants et de développer de nouvelles offres. Cela inclut les statistiques sur les produits et les marchés, les recherches et analyses, les benchmarks et autres analyses visant à mieux comprendre vos besoins et ceux des utilisateurs dans leur ensemble, à diagnostiquer les problèmes et à analyser les tendances.

7.2.4 2.4 Pour protéger nos Services et défendre nos droits ou ceux de tiers

Nous traitons vos données personnelles afin de garantir la sécurité et la fiabilité du Service. Cela inclut la détection, la prévention et la réponse aux fraudes, abus, risques de sécurité et problèmes techniques susceptibles de nuire à MyQ, à nos clients et aux utilisateurs finaux.

Nous pouvons traiter certaines des données spécifiées dans la section 1.1 lorsque la loi l'exige ou pour établir, exercer ou défendre nos droits légaux ou, si nécessaire, protéger les droits et intérêts de MyQ.

7.2.5 2.5 À des fins de marketing et de vente

Nous pouvons traiter les coordonnées des personnes de contact désignées par vous ou vos utilisateurs finaux afin de vous fournir des informations relatives aux nouvelles fonctionnalités des Services et aux nouvelles offres de produits. Pour plus de détails, veuillez consulter la section 7 ci-dessous.

7.3 3. Base juridique

Aux fins spécifiées aux sections 2.1 et 2.2, nous traitons vos données personnelles sur la base de notre contrat avec vous (si vous êtes notre client direct et une personne physique) ou sur la base de notre intérêt légitime à fournir nos Services à nos clients (lorsque notre client est votre entreprise ou organisation et que vous êtes un utilisateur final autorisé désigné par votre entreprise ou organisation).

Aux fins spécifiées à la section 2.3, nous traitons vos données personnelles sur la base de notre intérêt légitime à développer et améliorer nos Services.

Aux fins spécifiées dans la section 2.4, nous traitons vos données personnelles sur la base de notre intérêt légitime à protéger et à sécuriser nos droits ou revendications ou les droits de nos clients ou utilisateurs.

Aux fins spécifiées à la section 2.5, nous traitons vos données personnelles sur la base de votre consentement volontaire lorsque vous nous avez donné ce consentement. Dans une mesure limitée autorisée par la loi applicable, nous pouvons également utiliser vos coordonnées électroniques pour vous informer de nos Services sans votre consentement explicite, sur la base de notre intérêt légitime, comme décrit plus en détail à la section 7 ci-dessous.

Lorsque nous utilisons vos données personnelles pour nos intérêts légitimes, nous veillons à prendre en compte tout impact potentiel que cette utilisation pourrait avoir sur vous. Nos intérêts légitimes ne prévalent pas automatiquement sur les vôtres et nous n'utiliserons pas vos informations si nous estimons que vos intérêts doivent prévaloir sur les nôtres, sauf si nous avons d'autres motifs de le faire (tels que l'exécution d'un contrat, votre consentement ou une obligation légale). Si vous avez des inquiétudes concernant notre traitement, veuillez vous reporter aux détails de la section 9 ci-dessous intitulée « Vos droits ».

7.4 4. Périodes de conservation

Lorsque nous traitons des données à caractère personnel en tant que responsable du traitement, nous conservons vos données à caractère personnel pendant la durée nécessaire à la réalisation des finalités décrites dans la présente politique de confidentialité et/ou dans tout contrat de services, sauf si une conservation plus longue est requise par la loi (par exemple à des fins fiscales ou comptables ou en raison d'autres exigences légales) ou si le stockage des données est nécessaire pour la constatation, l'exercice ou la défense des droits légaux de MyQ ; dans ce cas, nous ne conserverons que les données nécessaires à l'exécution de nos droits ou à notre défense pendant la durée nécessaire dans le cas donné et sans dépasser les délais de prescription légaux.

Lorsque nous traitons des données à caractère personnel pour le compte de nos clients en tant que sous-traitant, nous conservons ces données pendant toute la durée de notre contrat avec ces clients et les supprimons automatiquement conformément à nos processus de conservation et de sauvegarde dans les 90 jours

suivant la résiliation du contrat, sauf si les clients nous demandent de les effacer plus tôt.

7.5 5. Partage de vos données à caractère personnel à des fins juridiques et commerciales

Nous pouvons utiliser et/ou divulguer à des tiers (y compris des organismes gouvernementaux et des autorités chargées de l'application de la loi, nos filiales, nos conseillers professionnels et nos fournisseurs ou sous-traitants) des informations vous concernant lorsque :

- Nous nous conformons à une procédure judiciaire ;
- Nous faisons valoir ou défendons les droits légaux de MyQ, et dans le cadre d'une restructuration d'entreprise telle qu'une fusion, une acquisition d'entreprise ou une situation d'insolvabilité ;
- Prévenir une fraude ou un préjudice imminent ; et
- Garantir la sécurité et le bon fonctionnement de notre réseau et de nos services.

Ces informations seront partagées à condition que, dans toutes ces circonstances, nous ne partagions que les informations personnelles limitées qui doivent être partagées dans cette situation particulière.

Nous partageons vos données avec nos partenaires commerciaux de confiance ou des personnes qui traitent vos données en tant que sous-traitants pour notre compte et conformément à nos instructions, conformément à la présente politique de confidentialité. Nous sélectionnons nos fournisseurs avec le plus grand soin et nous nous assurons toujours qu'ils fournissent une protection adéquate des données et des garanties de sécurité. À cet effet, nous avons lié nos sous-traitants à des accords de traitement des données conclus conformément à l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (« RGPD »).

Si vous sélectionnez dans l'interface d'administration MyQ que votre tenant de services soit situé dans l'UE, vos données client seront alors traitées dans l'UE, conformément aux engagements contractuels de Microsoft en matière de limites de données dans l'UE. Si vous sélectionnez votre locataire de services dans l'interface d'administration MyQ pour qu'il soit situé en dehors de l'UE, ce transfert sera effectué sur la base des clauses contractuelles types (clauses modèles) approuvées

par la Commission européenne (2010/87/UE), à moins qu'un autre mécanisme de transfert prévu aux articles 45, 46 et suivants du RGPD ne soit disponible. Nonobstant ce qui précède, vos données client peuvent également être transférées vers des pays pour lesquels la Commission européenne a rendu une décision d'adéquation.

Liste de nos sous-traitants actuels qui peuvent avoir accès à vos données personnelles :

- http://salesforce.comEMEA Ltd. (traitement lié aux ventes et assistance technique),
- Microsoft Ireland Operations Limited (collaboration et communication, Microsoft Azure – services d'hébergement cloud),
- TeamViewer GmbH (assistance technique).

Outre les sous-traitants mentionnés ci-dessus, nous pouvons également partager vos données personnelles afin de gérer nos processus commerciaux et de nous conformer à nos obligations légales, notamment en matière de logistique, de facturation, de fiscalité, de services juridiques et techniques.

Outre les fournisseurs tiers, MyQ peut partager des données avec ses filiales situées dans l'UE et au Royaume-Uni à des fins de services logistiques, de facturation, fiscaux, juridiques et techniques. La liste mise à jour de nos filiales dans l'UE et au Royaume-Uni est disponible à l'adresse https://www.myq-solution.com/en/the-list-of-myq-data-processors .

7.6 6. Statistiques anonymes

Nous pouvons utiliser des données agrégées anonymisées dérivées des données personnelles que vous nous avez fournies ou collectées par les analyses du programme, telles que le comportement et les activités des utilisateurs, pour nos propres statistiques, pour des audits, à des fins d'études de produits et de marché, pour des analyses (qui nous aident à optimiser et à améliorer nos Services et leur facilité d'utilisation, la gamme de Services et à développer de nouvelles technologies, produits et services), et pour des benchmarks et autres analyses.

7.7 7. Communications marketing

Nous pouvons contacter les personnes de contact désignées par vous ou vos utilisateurs finaux afin de leur fournir des informations relatives aux nouvelles fonctionnalités des Services et aux nouvelles offres de produits, à condition que nous disposions de l'autorisation nécessaire pour le faire, soit sur la base de votre

consentement (lorsque nous vous l'avons demandé et que vous nous l'avez donné), soit sur la base de nos intérêts légitimes à vous fournir des communications marketing lorsque nous pouvons le faire légalement, dans les limites prévues par la loi. Dans ce dernier cas, nous ne vous enverrons des communications marketing que si vous utilisez ou avez récemment utilisé l'un de nos Services et que vous ne vous êtes pas opposé à la réception de ces informations (par l'un des moyens mentionnés ci-dessous).

Vous pouvez modifier vos préférences en matière de communications marketing à tout moment en suivant les instructions ci-dessous :

- Si vous souhaitez vous désabonner d'un e-mail qui vous a été envoyé, suivez le lien « se désabonner » et/ou les instructions figurant au bas de l'e-mail.
- Vous pouvez également nous contacter en utilisant les coordonnées figurant dans la section « Contactez-nous » ci-dessous pour modifier vos préférences en matière de communications marketing, y compris pour retirer votre consentement.

Si vous avez reçu des e-mails indésirables et non sollicités envoyés via notre système ou prétendant être envoyés via notre système, veuillez transmettre une copie de cet e-mail avec vos commentaires à info@myq-solution.com[1] pour examen.

Veuillez noter que nous pouvons occasionnellement vous envoyer des informations importantes (y compris par e-mail) concernant les Services que vous utilisez ou avez utilisés, notamment des modifications des conditions générales applicables et/ou d'autres communications ou notifications pouvant être nécessaires pour remplir nos obligations légales et contractuelles, comme décrit dans la section 2.2 ci-dessus. Ces communications importantes relatives aux Services ne constituent pas des communications marketing et ne sont pas affectées par vos préférences.

7.8 8. Sécurité et emplacement de vos données

Nous avons mis en place et maintiendrons des mesures techniques et organisationnelles appropriées, des contrôles internes et des routines de sécurité de l'information conformément aux bonnes pratiques du secteur, tout en tenant compte de l'état du développement technologique, afin de protéger vos données contre toute perte accidentelle, destruction, altération, divulgation ou accès non autorisé ou destruction illégale. Ces mesures peuvent inclure, sans s'y limiter, la prise de mesures raisonnables pour garantir la fiabilité des employés ayant accès à vos données et la mise en place de droits d'accès limités et de contrôles d'accès ;

1. mailto:info@myq-solution.com

l'authentification ; la formation du personnel ; la sauvegarde régulière ; les procédures de récupération des données et de gestion des incidents ; les restrictions relatives au stockage, à l'impression et à l'élimination des données à caractère personnel ; la protection logicielle des périphériques sur lesquels sont stockées les données à caractère personnel ; etc.

7.9 9. Vos droits

Cette section décrit vos droits en vertu des lois applicables, telles que le RGPD, et la manière de les exercer. Si vous exercez l'un de vos droits en vertu de cette section ou des lois applicables, nous communiquerons toute rectification ou suppression de vos données personnelles ou toute restriction de traitement effectuée conformément à votre demande à chaque destinataire auquel les données personnelles ont été divulguées conformément à la section 5 de la présente politique de confidentialité, à moins que cette communication s'avère impossible ou implique un effort disproportionné.

Si vous souhaitez exercer ces droits et/ou obtenir toutes les informations pertinentes concernant le traitement de vos données personnelles, veuillez nous contacter à l'adresse[2] info@myq-solution.com[3]. Il vous sera demandé de vous identifier ; cela est nécessaire pour vérifier que la demande a bien été envoyée par vous. Nous vous répondrons dans un délai d'un mois après réception de votre demande, mais nous nous réservons le droit de prolonger ce délai jusqu'à deux mois dans des circonstances exceptionnelles justifiées. Dans tous les cas, nous vous informerons dans un délai d'un mois après réception de votre demande si nous décidons de prolonger le délai de réponse.

Conformément aux lois applicables et comme décrit plus en détail ci-dessous, vous avez le droit de demander l'accès à vos données personnelles et aux informations relatives à leur traitement, le droit de rectification, d'effacement ou de portabilité (par exemple, le transfert de vos données personnelles vers un autre prestataire de services) des données personnelles que nous traitons, ainsi que le droit de vous opposer au traitement de vos données personnelles et/ou de demander la limitation de ce traitement.

Veuillez noter que votre opposition au traitement pourrait nous empêcher de vous fournir nos services ou d'effectuer les actions nécessaires pour atteindre les objectifs énoncés ci-dessus (voir la section 2 « Comment nous utilisons les données »).

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

Il est important que les données personnelles que nous détenons à votre sujet soient exactes et à jour. Veuillez nous tenir informés si vos données personnelles changent au cours de votre relation avec nous en nous contactant via les coordonnées indiquées à la section 10 « Contactez-nous ».

7.9.1 9.1 Informations sur vos données personnelles, accès à celles-ci et rectification de celles-ci

Conformément aux lois applicables, vous avez le droit d'obtenir la confirmation que des données à caractère personnel vous concernant sont ou ne sont pas traitées (conformément au processus décrit ci-dessus) et, le cas échéant, le droit d'accéder à vos données à caractère personnel que vous avez partagées avec nous et de les rectifier. Grâce aux paramètres des Services, vous pouvez accéder à vos informations de compte, les mettre à jour et modifier les paramètres de votre profil.

7.9.2 9.2 Exactitude de vos données personnelles

Nous prenons des mesures raisonnables pour nous assurer que vous pouvez maintenir vos données personnelles exactes et à jour. Vous pouvez toujours nous contacter afin d'obtenir la confirmation que nous traitons toujours ou non vos données personnelles.

Si vous constatez que vos données personnelles traitées par nos soins sont inexactes ou incomplètes et que vous ne parvenez pas à les mettre à jour conformément à la section 9.1 de la présente Politique de confidentialité, vous pouvez nous demander de mettre à jour ces données personnelles. Nous vérifierons votre identité et mettrons à jour vos données personnelles en votre nom.

7.9.3 9.3 Effacement de vos données personnelles

Vous pouvez nous demander d'effacer vos données personnelles à tout moment. Si vous nous adressez une telle demande, nous supprimerons toutes vos données personnelles en notre possession sans délai injustifié, à condition que vos données personnelles ne soient plus nécessaires à la fourniture des Services ou à d'autres fins autorisées, notamment en rapport avec l'exercice et la défense de nos droits légaux ou le respect de nos obligations légales. Nous supprimerons également (et veillerons à ce que les sous-traitants auxquels nous faisons appel suppriment) toutes vos données personnelles si vous retirez votre consentement ou si la loi nous y oblige.

7.9.4 9.4 Limitation du traitement

Si vous nous demandez de limiter le traitement de vos données personnelles, par exemple lorsque vous contestez l'exactitude, la légalité ou la nécessité du traitement de vos données personnelles, nous limiterons le traitement de vos données personnelles au minimum nécessaire (stockage) et, le cas échéant, nous les traiterons uniquement pour la constatation, l'exercice ou la défense de droits en justice ou, si nécessaire, pour la protection des droits d'une autre personne physique ou morale, ou pour d'autres raisons limitées dictées par la loi applicable. Si la limitation est levée et que nous continuons à traiter vos données à caractère personnel, vous en serez informé sans retard injustifié.

7.9.5 9.5 Portabilité de vos données à caractère personnel

Vous avez le droit de recevoir les données à caractère personnel vous concernant et que vous nous avez fournies. Si vous nous adressez une telle demande, nous vous fournirons vos données à caractère personnel dans un format couramment utilisé et lisible par machine, sans retard injustifié à compter de la réception de votre demande. Si vous en faites la demande, nous enverrons vos données à caractère personnel à un tiers (un autre responsable du traitement) que vous identifierez dans votre demande, à moins que cette demande ne porte atteinte aux droits ou libertés d'autrui et que cela soit techniquement possible.

7.9.6 9.6 Opposition au traitement

Vous avez le droit de vous opposer à l'utilisation de vos données personnelles sur la base de nos intérêts légitimes. Dans ce cas, nous ne traiterons plus vos données personnelles, sauf si nous démontrons des motifs légitimes et impérieux pour leur traitement ultérieur qui prévalent sur vos intérêts, droits et libertés, ou pour la constatation, l'exercice ou la défense de nos droits en justice. Si vous vous opposez au traitement de vos données à des fins de marketing direct, nous cesserons de traiter vos données à ces fins.

7.9.7 9.7 Retrait de votre consentement

Si vous nous avez donné votre consentement pour le traitement de données à caractère personnel, par exemple à des fins de communication marketing, vous pouvez retirer votre consentement à tout moment sans avoir à fournir de motif. Nous bloquerons vos données à caractère personnel pour tout traitement ultérieur.

Veuillez noter que le retrait de votre consentement n'affecte pas la licéité de tout traitement fondé sur le consentement avant son retrait.

7.9.8 9.8 Réclamation auprès d'une autorité de protection des données

Vous avez le droit de déposer une plainte concernant nos activités de traitement des données auprès de l'Úřad pro ochranu osobních údajů, à l'adresse Pplk. Sochora 2Z, 170 00 Praha 7, République tchèque.

7.9.9 9.9 Demande de désinscription de la vente de données personnelles en vertu de la CCPA

MyQ ne vend aucune donnée à caractère personnel au sens de la CCPA. Par conséquent, si un consommateur californien communique une demande de désinscription en vertu de cette disposition, celle-ci n'aura aucun effet. Si vous souhaitez obtenir des informations supplémentaires sur vos droits en vertu de la CCPA de vous désinscrire de la vente de vos données à caractère personnel, veuillez contacter : info@myq-solution.com[4].

7.10 10. Contactez-nous

Si vous avez des questions concernant nos pratiques en matière de collecte et de protection des données ou vos droits, n'hésitez pas à nous contacter à l'adresse info@myq-solution.com[5].

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

8 Disponibilité des serveurs, sauvegarde des données et reprise après sinistre

8.1 Disponibilité du serveur

MyQ Roger s'engage à maintenir un objectif de disponibilité de 99,9 % ; toutefois, les accords de niveau de service (SLA) sont adaptés à chaque client et ne garantissent pas explicitement cet objectif. Nous utilisons des stratégies avancées de haute disponibilité (HA), en tirant parti de déploiements multizones et d'architectures multipods afin d'assurer la continuité du service et de minimiser les temps d'arrêt potentiels en cas de perturbations opérationnelles.

8.2 Surveillance en temps réel de l'état du système

Afin d'améliorer la transparence et d'offrir une visibilité en temps réel sur les performances du système, nous maintenons un site dédié qui fournit des informations actualisées sur l'état du service. Cette plateforme permet aux clients de :

- **Surveiller l'état du système en direct** : consulter les indicateurs opérationnels en temps réel et les mises à jour sur les incidents.
- **Recevoir des notifications proactives** : s'abonner à des alertes en cas de dégradation du service ou d'événements de maintenance planifiés.
- **Accéder aux rapports historiques sur la disponibilité** : examiner les incidents passés et les tendances en matière de performances afin d'évaluer la fiabilité.

En proposant un site centralisé dédié à l'état du système, nous fournissons à nos clients des informations précises et actualisées, ce qui renforce leur confiance et leur permet de prendre des décisions proactives en cas de perturbations.

8.3 Stratégies de sauvegarde

8.3.1 Stratégie de sauvegarde Azure SQL

Nous utilisons une stratégie de sauvegarde géo-redondante pour les bases de données Azure SQL, garantissant la résilience et la récupérabilité des données. Les aspects clés sont les suivants :

- **Stockage géo-redondant** : les sauvegardes sont répliquées dans plusieurs régions à des fins de reprise après sinistre.
- **Politique de conservation** : les sauvegardes sont conservées pendant plusieurs mois, ce qui permet la récupération des données historiques.

- **Sauvegardes incrémentielles** : une fenêtre de récupération ponctuelle (PITR) de 14 jours permet une restauration granulaire des données perdues.
- **Personnalisation basée sur les SLA** : les périodes de conservation et les objectifs de temps de récupération (RTO) varient en fonction des SLA spécifiques au cluster et peuvent être adaptés aux besoins des clients.

8.3.2 Stratégie de sauvegarde Azure Cosmos DB

Pour Azure Cosmos DB, nous mettons en œuvre des mécanismes complets de protection des données, en particulier pour les enregistrements comptables, afin de garantir l'intégrité et la traçabilité des données :

- **Rapports complets sur les données comptables** : toutes les transactions comptables, y compris la comptabilité des travaux d'impression, de numérisation, de copie et de télécopie, sont entièrement enregistrées.
- **Retracement des données historiques** : notre système permet de suivre et de retracer tous les enregistrements comptables signalés afin de garantir la conformité et l'auditabilité.
- **Haute disponibilité et redondance** : la réplication multirégionale embarquée garantit la continuité et minimise les risques de perte de données.

En mettant en œuvre ces stratégies de sauvegarde robustes, nous protégeons les données commerciales critiques tout en offrant des options de récupération flexibles adaptées aux accords de niveau de service (SLA) spécifiques à chaque client.

8.4 Scénarios de catastrophe et plan d'intervention

Scénario de catastrophe	Stratégie d'atténuation	Processus de récupération
Corruption des données	PITR (restauration à un instant donné)	Restauration de la base de données à son dernier état connu
Panne de la région cloud	Sauvegardes géo-redondantes et basculement	Passage à la région Azure secondaire
Défaillance du nœud Kubernetes	Réplication automatique des services dans AKS	Les pods sont reprogrammés vers des nœuds sains
Cyberattaque (DDoS, ransomware, etc.)	WAF, protection Azure DDoS et surveillance de la sécurité	Isolation des systèmes compromis, restauration à partir de sauvegardes saines

9 Zéro confiance

9.1 Comprendre la sécurité Zero Trust

La confiance est une notion complexe. Par exemple, je fais confiance à ma mère pour préparer un dîner parfait, mais je ne lui confierais jamais la sécurité du réseau. En matière de cybersécurité, une confiance mal placée peut entraîner des vulnérabilités importantes, c'est pourquoi le modèle Zero Trust existe.

9.1.1 Exemple concret : le danger de la confiance implicite

L'une des violations les plus connues où l'absence de principes Zero Trust a joué un rôle est l'**attaque** contre **Colonial Pipeline** en 2021. Les attaquants ont obtenu l'accès grâce à des identifiants VPN compromis, qui n'étaient pas protégés par une authentification multifactorielle (MFA). Comme le réseau faisait implicitement confiance aux utilisateurs authentifiés, les attaquants ont pu se déplacer latéralement et déployer un ransomware, provoquant une pénurie généralisée de carburant à travers les États-Unis. Cet incident montre pourquoi « ne jamais faire confiance, toujours vérifier » est essentiel à la cybersécurité moderne.

9.2 Qu'est-ce que le Zero Trust ?

Le Zero Trust est un paradigme de cybersécurité fondé sur le principe « ne jamais faire confiance, toujours vérifier ». Il garantit que les utilisateurs et les périphériques ne sont pas considérés comme fiables par défaut, même s'ils sont connectés à un réseau d'entreprise sécurisé ou ont déjà été vérifiés. Au contraire, la confiance doit être continuellement évaluée et validée sur la base de divers signaux de sécurité.

9.2.1 Les principes fondamentaux du Zero Trust

Le Zero Trust est défini dans **la norme NIST SP 800-207** comme un cadre axé sur la protection des ressources grâce à une vérification continue. Ce modèle de sécurité s'applique à :

- **Gestion des identités et des accès** : garantir l'authentification sécurisée des utilisateurs et des périphériques.
- **Sécurité du réseau et des terminaux** : protéger les communications et appliquer des contrôles d'accès stricts.
- **Protection des données** : garantir que les données sensibles sont cryptées et stockées en toute sécurité.

- **Surveillance continue** : détecter les anomalies et répondre aux menaces potentielles en temps réel.

9.3 Comment le Zero Trust s'applique à MyQ Roger

9.3.1 Vérification explicite

- L'authentification est requise même sur les périphériques autorisés (téléphones/ordinateurs de bureau).
- Utilisation de normes d'authentification modernes.
- L'authentification multifactorielle (MFA) est appliquée pour les connexions mobiles et les imprimantes multifonctions (MFP).
- Le flux OAuth2 Device Flow est mis en œuvre pour l'autorisation des périphériques.
- **Des mécanismes d'authentification continue** suivent les changements dans le comportement des utilisateurs afin de détecter les anomalies.

9.3.2 Gestion des accès

- **Le contrôle d'accès basé sur les rôles (RBAC)** garantit que les utilisateurs ne disposent que de l'accès minimum nécessaire.
- **Le principe du moindre privilège** est appliqué afin de réduire les risques de sécurité.
- **La micro-segmentation** est mise en œuvre pour limiter les mouvements latéraux au sein du réseau.
- **Les contrôles d'accès juste à temps (JIT)** ajustent dynamiquement les privilèges des utilisateurs en fonction du contexte.

9.3.3 Sécurité des périphériques et des terminaux

- Des jetons d'accès uniques sont émis pour chaque type de périphérique.
- Le protocole TLS (Transport Layer Security) est obligatoire pour toutes les communications.
- **Les solutions de détection et de réponse aux incidents au niveau des terminaux (EDR)** surveillent et analysent le comportement des périphériques.
- **L'accès réseau zéro confiance (ZTNA)** garantit que seuls les périphériques autorisés peuvent accéder à des ressources spécifiques.

9.3.4 Protection des données

- Toutes les données sont stockées de manière sécurisée à l'aide de solutions de stockage cryptées.
- Des politiques garantissent que seules les entités autorisées peuvent accéder aux données.

- **Les solutions de prévention des pertes de données (DLP)** surveillent et empêchent l'exfiltration non autorisée de données.
- **Les enclaves sécurisées** protègent les données hautement sensibles contre tout accès non autorisé.

9.4 Lutter contre les cybermenaces avec le modèle Zero Trust

Le modèle Zero Trust permet d'atténuer les menaces suivantes :

- **Menaces internes** : empêche les employés ou les comptes compromis d'obtenir un accès non autorisé.
- **Attaques par credential stuffing et phishing** : réduit l'impact des identifiants compromis grâce à une authentification continue.
- **Attaques par mouvement latéral** : la micro-segmentation empêche les attaquants de se déplacer latéralement sur les réseaux.
- **Attaques de la chaîne d'approvisionnement** : garantit une vérification stricte des accès et des intégrations de tiers.

9.5 Considérations en matière de conformité et de réglementation

Zero Trust s'aligne sur diverses réglementations et cadres de cybersécurité :

- **ISO 27001** : impose une gestion sécurisée des accès et la protection des données.
- **RGPD** : garantit le traitement et le stockage sécurisés des données personnelles.
- **HIPAA** : protège les informations sensibles relatives aux soins de santé.
- **Cadre de cybersécurité du NIST** : fournit des lignes directrices pour la mise en œuvre du Zero Trust.

9.6 Pourquoi le Zero Trust est-il important ?

L'adoption du Zero Trust minimise les risques de failles de sécurité, de menaces internes et d'accès non autorisés. À une époque où les cybermenaces sont de plus en plus nombreuses, une architecture Zero Trust offre une protection robuste en garantissant une vérification continue et des contrôles d'accès stricts sur toutes les ressources.

En mettant en œuvre ces principes, MyQ Roger garantit une posture de sécurité sécurisée, résiliente et adaptative, conforme aux meilleures pratiques modernes en matière de cybersécurité. De plus, la surveillance continue, les contrôles d'accès et la détection des menaces en temps réel renforcent la capacité de l'organisation à répondre efficacement aux cybermenaces en constante évolution.

10 Connexion sécurisée avec MyQ Roger

10.1 Introduction

L'utilisation d'un code PIN comme principale méthode de connexion n'a jamais été vraiment sécurisée. Les premiers téléphones mobiles reposaient sur des codes PIN, mais à mesure que les préoccupations en matière de sécurité ont évolué, les méthodes d'authentification ont également évolué. Aujourd'hui, la biométrie est devenue la norme, offrant une approche plus sécurisée et plus conviviale de l'authentification.

MyQ Roger s'inscrit dans cette évolution en mettant en œuvre la dernière version de l'OAuth 2.0 Device Authorization Grant (anciennement connu sous le nom de Device Flow). Cette méthode d'authentification moderne exige que les utilisateurs se connectent à l'aide d'un code QR à usage unique scanné avec leur téléphone mobile, éliminant ainsi le besoin de mots de passe statiques ou de codes PIN peu sûrs.

Nous considérons le téléphone portable d'un utilisateur comme l'un des moyens d'authentification les plus sûrs. En utilisant l'authentification biométrique pour déverrouiller le téléphone et accéder ensuite à l'application MyQ, nous nous assurons que la personne qui se connecte est bien le propriétaire légitime du compte.

10.2 Authentification sécurisée avec MyQ Roger

- **Autorisation d'appareil OAuth 2.0** : au lieu de s'appuyer sur les codes PIN traditionnels, les utilisateurs s'authentifient à l'aide d'un code QR généré dynamiquement. Cette méthode réduit considérablement le risque de vol d'identifiants ou d'attaques par réutilisation.
- **Vérification biométrique** : les smartphones modernes nécessitant une vérification biométrique (par exemple, empreinte digitale ou reconnaissance faciale) pour être déverrouillés, cela ajoute un niveau de sécurité supplémentaire avant d'accéder à MyQ Roger.

10.3 Authentification par code PIN hérité

Bien que MyQ Roger propose toujours la connexion par code PIN en option, cette méthode est considérée comme peu sûre et est déconseillée par défaut. Les utilisateurs qui choisissent d'activer l'authentification par code PIN doivent explicitement la marquer comme sûre, en reconnaissant les risques de sécurité associés. De plus, l'activation de la connexion par code PIN désactivera certaines fonctionnalités de sécurité avancées afin d'atténuer les vulnérabilités potentielles.

10.4 Responsabilité en matière de sécurité

Si une organisation choisit d'autoriser la connexion par code PIN, la responsabilité du maintien d'un environnement sécurisé incombe au client. Les meilleures pratiques telles que l'application de politiques strictes en matière de codes PIN, la mise en œuvre de mesures de sécurité physiques et la surveillance des journaux d'accès doivent être suivies afin de minimiser les risques.

10.5 Conclusion

Avec MyQ Roger, nous accordons la priorité à la sécurité en tirant parti des normes d'authentification modernes. L'adoption de l'authentification biométrique sur mobile garantit une expérience utilisateur fluide et sécurisée. Bien que la connexion par code PIN traditionnelle reste disponible, elle n'est pas la méthode recommandée et les clients doivent prendre des précautions supplémentaires s'ils choisissent de l'utiliser. En adoptant des mécanismes de connexion sécurisés, les organisations peuvent améliorer à la fois la sécurité et la convivialité pour leurs utilisateurs.

11 Impression sécurisée avec MyQ Roger

11.1 Le défi de l'impression sécurisée

Les méthodes traditionnelles d'impression sécurisée reposent sur des connexions physiques, telles que des câbles LPT, où une imprimante dédiée est attribuée à un seul ordinateur portable. Si cette méthode garantit le plus haut niveau de sécurité, elle n'est pas pratique dans les environnements modernes qui exigent flexibilité, mobilité et partage des ressources.

AirPrint et Mopria offrent des fonctionnalités d'impression sécurisée, mais sont insuffisantes dans les cas où les utilisateurs peuvent lancer des travaux d'impression à distance sans être physiquement présents à proximité de l'imprimante. Cela crée des failles de sécurité, les documents sensibles pouvant être laissés sans surveillance.

11.2 MyQ Roger : une solution d'impression sécurisée complète

MyQ Roger intègre plusieurs flux de travail d'impression tout en appliquant des protocoles de sécurité pour garantir que les utilisateurs doivent être physiquement présents pour authentifier et lancer les travaux d'impression. Le système garantit que les travaux d'impression sont stockés et transmis de manière sécurisée tout en minimisant l'exposition des données.

11.3 Méthodes d'impression sécurisées dans MyQ Roger

11.3.1 1) Impression directe du PC à l'imprimante

- Utilise **le protocole IPP/s (Internet Printing Protocol Secure)** pour transférer les travaux d'impression en toute sécurité.
- Marques d'imprimantes prises en charge : **Ricoh, Kyocera**.
- Les travaux d'impression restent stockés directement sur l'imprimante jusqu'à ce que l'utilisateur s'authentifie et lance le travail.

11.3.2 2) MyQ Roger Client (MRC)

- Les travaux d'impression sont **cryptés et stockés localement** sur le PC de l'utilisateur.
- L'imprimante **ne** récupère le fichier crypté **qu'après authentification de l'utilisateur**.
- L'impression sécurisée est exécutée via **IPP/s**.

11.3.3 3) Impression dans le cloud

- Les fichiers d'impression sont stockés en toute sécurité dans le stockage cloud de l'utilisateur (par exemple, **OneDrive, Google Drive, Dropbox**).
- L'imprimante télécharge le document directement depuis le stockage cloud à l'aide d'un **lien d'accès à durée limitée**.
- **Aucun document n'est conservé** sur l'imprimante après l'impression, ce qui garantit la confidentialité des données.

11.3.4 4) Intégration Microsoft Universal Print

- MyQ Roger met en œuvre un **connecteur d'impression universel** qui permet aux imprimantes de communiquer directement avec **les serveurs d'impression universels de Microsoft**.
- Les travaux d'impression sont stockés en toute sécurité sur **les serveurs Microsoft** et récupérés à la demande après authentification de l'utilisateur.
- L'impression est effectuée via **les pilotes Universal Print**, ce qui garantit un traitement fluide et sécurisé des travaux.

11.4 Conclusion

MyQ Roger offre un **environnement d'impression holistique et sécurisé** en combinant des flux de travail d'impression directs, locaux et basés sur le cloud avec des mesures de sécurité robustes. En exigeant que les utilisateurs s'authentifient en personne avant l'exécution des travaux, MyQ Roger élimine les risques associés aux travaux d'impression sans surveillance, garantissant une protection maximale des données dans les environnements de travail modernes.

12 Contacts professionnels

Fabricant MyQ®	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prague 9, République tchèque Numéro d'identification 615 06 133 MyQ® spol. s r.o. est inscrite au registre du commerce du tribunal municipal de Prague, sous le numéro C 29842 (ci-après dénommée « MyQ® »)
Informations commerciales	http://www.myq-solution.com info@myq-solution.com[6]
Assistance technique	support@myq-solution.com[7]
Avis	LE FABRICANT NE PEUT ÊTRE TENU RESPONSABLE DE TOUTE PERTE OU DOMMAGE RÉSULTANT DE L'INSTALLATION OU DU FONCTIONNEMENT DES COMPOSANTS LOGICIELS ET MATÉRIELS DE LA SOLUTION D'IMPRESSION MyQ®. Ce manuel, son contenu, sa conception et sa structure sont protégés par le droit d'auteur. La copie ou toute autre reproduction de tout ou partie de ce guide, ou de tout élément protégé par le droit d'auteur, sans l'accord écrit préalable de MyQ® est interdite et peut être punie par la loi. MyQ® n'est pas responsable du contenu de ce manuel, notamment en ce qui concerne son intégrité, sa monnaie et son occupation commerciale. Tout le matériel publié ici est exclusivement à titre informatif. Ce manuel est susceptible d'être modifié sans préavis. MyQ® n'est pas tenu d'effectuer ces modifications périodiquement ni de les annoncer, et n'est pas responsable de la compatibilité des informations actuellement publiées avec la dernière version de la solution d'impression MyQ®.

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

Marques commerciales	« MyQ® », y compris ses logos, est une marque déposée de MyQ®. Toute utilisation des marques commerciales de MyQ®, y compris ses logos, sans l'accord écrit préalable de MyQ® Company est interdite. La marque commerciale et le nom du produit sont protégés par MyQ® et/ou ses filiales locales.

myQ roger

GAGNEZ DU TEMPS GRÂCE À DES SOLUTIONS D'IMPRESSION PERSONNALISÉES

MyQ Roger est une solution cloud-native conçue pour les bureaux modernes privilégiant le cloud, simplifiant les flux de travail documentaires et permettant une navigation, une impression et une numérisation sécurisées où que se trouvent les utilisateurs.

info@myq-solution.com

myq-solution.com

+ de 50 millions
d'utilisateurs nous font confiance

+d'1 million
d'équipements actifs

26+ marques
supportées

1000+
Partenaires certifiés

Présent dans
+ de 140 pays

Récompensé et certifié

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001