

A GUIDE TO GDPR COMPLIANCE

*Implementing Your Print
System for GDPR*



by MyQ Solution

04.01.2018

myQ



Contents

1. What is GDPR
2. Why secured print management systems
3. MyQ GDPR compliance
4. The path to compliance
5. Conclusion



1. WHAT IS GDPR

Implementing Your Print System for GDPR

The General Data Protection Regulation (GDPR) is set to go into effect on 25 May 2018 and this new, enforceable law will have far-reaching global implications on organizations that control the personal data of their customers and employees.

GDPR aims to protect how personal data is stored, processed, and destroyed after it's no longer needed. This allows EU citizens to gain better control over the way their personal data is being used.

GDPR is binding and applicable at the EU level, rather than requiring legislation on behalf of individual state governments. It is an upgrade from the outdated data protection directive of 1995.

To fulfill these new regulations, GDPR has introduced some new terms that apply to data-collecting organizations. These terms include:

Data Controller – the entity that controls the purposes, conditions and means of personal data.

Data Subject – the person whose data is being held.

Data Processor – any organization that processes personal data for the data controller.

Companies that fail to comply with the new regulations will face harsh penalties that include a maximum fine of €20 million or four percent of their annual global turnover, whichever is more.

For organizations, GDPR marks a shift away from programmatic audience targeting. GDPR will give organizations the mandated opportunity to increase their cyber security in order to mitigate potential breaches.

In this process of securing data, organizations must also acknowledge the rights of human data subjects, specifically in the areas of notifying involved parties of a breach, the means of storing and having access to the data, as well as the policies for data deletion.

2.)

WHY SECURED PRINT MANAGEMENT SYSTEMS

Directive 95/46/EC was intended to bring together the laws of different member states, but it left much room for interpretation. Meanwhile, the world of IT and data information was changing rapidly. GDPR aims to adapt to these changes.

Organizations that handle the personal data of their customers and employees need to have a secure printing system, otherwise organizations are susceptible to data loss from unsecured documents and cyber-attacks. There are procedures that organizations can implement to reduce the chance of losing personal data and ensure that they meet GDPR compliance regulations.

GDPR means...

- Organizations need to better secure consumer and employee data
- People are granted more control of their data
- Employee data must be able to be erased upon request

- MyQ server operates securely behind your firewall and all data is encrypted
- Tasks sent across your MyQ server are encrypted—only admin and the user have access
- Users can access all devices via ID card, PIN, or mobile
- All print jobs are stored at the MyQ server in a predefined folder and can be set to be deleted automatically
- MyQ Audit Log saves all changes at the admin level

3.) MYQ GDPR COMPLIANCE

MyQ Solution streamlines the way you do business by securing sensitive documents, saving time, reducing waste, and lowering costs.

Present in more than 80 countries, MyQ supports more than 3600 devices from 26 vendors. MyQ meets or exceeds all aspects of your managed-print-service (MPS) requirements – from cost control to waste management to saving employees valuable time throughout their day – securely.

- MyQ 7.1 includes enhanced features that make GDPR compliance easier. Clients can easily anonymize users via encryption, display user data, or remove records.
- MyQ 7.1 watermarking includes computer name and IP address, raising employee awareness

4. THE PATH TO GDPR COMPLIANCE

A) *Secure your print system from the beginning*

Securing your print system from end to end means that the user's print process is secure from when they decide to print to when they retrieve the document. Data encryption helps secure the document while it is in the system, and security features such as pull printing make sure that documents are only printed by the people who requested the print job.

User data is doubly secured. MyQ server is safely stored behind your organization's firewall and all data is encrypted on the server network helping to prevent cyber attacks.

B) *Control your scans and data deletion*

Data loss isn't something that only occurs with physical documents. Cyberattacks can be a constant threat to organizations if they do not have a well-rounded security system in place. Secure scan is one way for organizations to prevent these attacks. After a file is scanned, it is stored on the server in a link sent by email. The scan is not accessible until the link is clicked from the email.

Another option to thwart cyberattacks is data deletion. If a print, scan, or copy job is left on a multifunctional device (MFD), administrators have the option of setting a time for when the jobs should automatically be deleted.

User data is easily erased. MyQ automates the change of personal information. If end users request their data to be deleted, it can be done with one click.

C) Secure documents with pull print and watermarking

Pull printing is widely recognized as an essential aspect of print management. Security procedures for pull printing allow documents to be printed only after an employee has entered a PIN code or swiped an ID card at the printer. This means that no unauthorized person can retrieve the printed documents from the device. This prevents sensitive documents from lying in the paper tray, allowing anyone to pick them up, intentionally or otherwise.

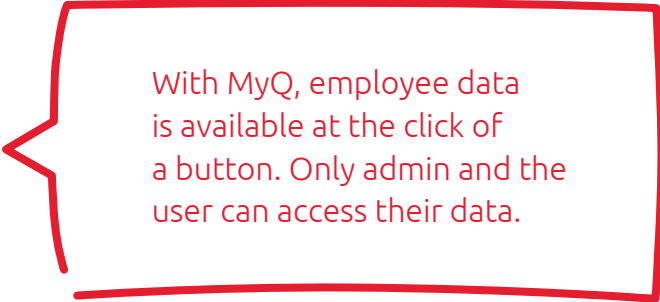
Another aspect of MPS to implement is watermarking pages with information about who printed the document, when and where it was printed. If employees know that this information is on printed documents, it can help them to have more self-awareness about keeping track of their paperwork.

MyQ 7.1 improved watermarking includes computer name and IP address. This helps to ensure that users safeguard sensitive documents and prevents information loss.



D) Provide the right to access

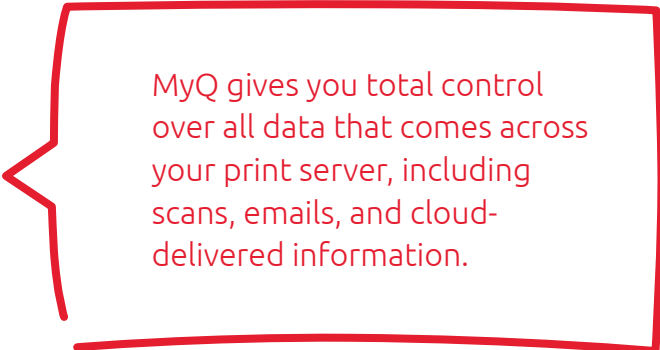
Under the GDPR, data subjects have a right to access, which means that they can acquire confirmation of their personal data if it is being processed, as well as where it is stored and why. The controller must also provide an electronic copy of the data, free of charge. MyQ's print management feature safely logs and encrypts the user's information, making it easily accessible upon request.

A red callout box with a pointed left side, containing text about data access.

With MyQ, employee data is available at the click of a button. Only admin and the user can access their data.

E) Provide the right to be forgotten

This aspect of GDPR allows data subjects to have the data controller erase their personal data, stop further distribution of their data, and even demand that third parties quit processing their data. For this to occur, the data must no longer be related to the original purpose of processing it. One example is when an ex-employee no longer wants their previous employer to store their personal details and printing history. If end users request their data to be deleted, MyQ makes it easy with one click.

A red callout box with a pointed left side, containing text about data deletion.

MyQ gives you total control over all data that comes across your print server, including scans, emails, and cloud-delivered information.

5. CONCLUSION

The EU is taking the issue of personal data security seriously, changing an earlier directive into a regulation. Customer data protection and security have been foundational objectives of MyQ since the company began. Some organizations may have trouble complying with GDPR, but MyQ is committed to helping our customers meet the regulations by providing easy-to-use, secure solutions.



“All the other solutions were expensive and very complicated to install, use and maintain. We had one definitive vision - to produce a simple and cost-effective solution.”

Martin Januš,
MyQ Chief Executive Officer

MyQ makes the award-winning, universal MyQ Solution for secure print management and workflow optimization via printers and other multi-functional devices.

myQ



Headquartered in Prague, Czech Republic, with additional branches in Austria, France, Germany, Russia, UAE, the UK, and the USA, MyQ works with the most-recognized global vendors in the printing industry. CIO rates MyQ a "Top 100" Czech technology company.

For more info, visit:

www.myq-solution.com

A GUIDE TO GDPR COMPLIANCE

Implementing Your Print System for GDPR



info@myq-solution.com
www.myq-solution.com
+420 228 800 697

Harfa Office Park
Českomoravská 2420/15
190 93 PRAGUE
CZECH REPUBLIC

Print less, scan more, focus on what you do best...

myq