GDPR Compliance Guide

For Print Management

by PaperCut Software – 29 January 2018

Make your Print System GDPR Compliant

The General Data Protection Regulation (GDPR) is enforceable from May 25, 2018, with stiff penalties for data breaches.

It applies globally to all organizations employing European Union (EU) residents that are collecting or processing personal data about that resident

GDPR is a major upgrade to data privacy regulations in the EU and is making waves worldwide, with many other jurisdictions adopting similar provisions.

The aim of the GDPR is to give control of EU residents' personal data back to the individual, and generally improve data privacy with a uniform set of regulations. Several new terms have been defined, including:

- "Data Controller"—an entity that holds and manages user data
- "Data Subject"—a person whose data is being held. A Data Subject is any identifiable person, and may be a prospect, a client, or an employee of your company.
- 'Data Processor'—an organization that processes data on behalf of a data controller (e.g. cloud service providers).

To comply with GDPR, organizations must ensure their information systems are secure. Data protection should be by design and by default. Organizations must also respect the rights of Data Subjects, ensuring they obtain consent to store information and to promptly notify authorities if a data breach occurs. Data Subjects must also be able on request to access their information and to have their information erased.

Why the Print System must be Secured

The foundation of a GDPR compliant system is a well designed and secure information system. The regulation raises the bar by stating that security should be designed in from the beginning, and that personal data should be anonymized wherever possible.

The print system is not exempt from these requirements. An unsecured print system can leave your organization vulnerable for two reasons:it is a point of entry for an attacker, and printed documents themselves can be a source of data loss. In a 2017 Quocirca report[1], more than 80% of companies report concerns about print related data losses, with 61% reporting actual losses in the past year.

About PaperCut

Papercut is a leading global provider of Print Management software with it's PaperCut NG and PaperCut MF product line.

With nearly 125,000 Multifunction and/or single function devices running PaperCut MF across the 28 European Union countries, we provide a trusted product to ensure that all requirements can be met from cost control through to enhanced productivity underpinned by a market leading security features.

Below are five practical steps you can take to have your printing system comply with GDPR requirements, and how PaperCut MF can help you achieve them...

[1] "Print in the digital age" Louella Fernandes, Quocirca 2017

5 Actionable Steps for GDPR Compliance

1. Secure your print system

Securing your print system is all about securing the end-to-end workflow from the time a user issues a print command through to the lifecycle of a printed document. Key infrastructure, such as print servers and network, need to be correctly secured. Print Management solutions, such as PaperCut NG and PaperCut MF, play an important role in helping build secure print infrastructure. PaperCut's Security WhitePaper[2] provides a clear guide on how to make your print system secure.

2. Stop unwanted printouts with Secure Print Release

It is not uncommon for organizations to throw away hundreds of documents left uncollected on printer trays each day. This is highly wasteful and the information in these documents is often private or confidential and should not be leaked. Secure Print Release is a simple and proven solution; documents are not actually printed until the user walks up to the printer and authenticates themselves. This feature alone will typically more than justify implementing a print management solution such as PaperCut MF, driving both a positive ROI & payback in conjunction with strong security enhancements.

3. Implement policies to protect printed documents

Even when a printed document is delivered into the hands of the intended recipient, thought should be given to what happens then. How are documents stored in the workplace and how are they disposed? Is confidential information being put at risk?

Often documents are taken outside the workplace, where the risk of information loss or a data privacy breach is higher. Employees should be trained to take appropriate care of printed material outside the office. If a mistake or breach occurs, it is important to be able to trace where and when the document was printed and by whom. The ability to trace a document source is also a strong incentive for users to take appropriate care.

[2] https://www.papercut.com/kb/Main/SecurityWhitepaper

Print Policy Example:

PaperCut NG and MF's watermarking and digital signature features provide exactly this tracing ability. The signature can be used to trace a printed document back to the entry in the print job log, which contains full details of the date, time, printer, and author of the print job.

4. Support a Data Subject's Right to Access their information

The GDPR requires that organizations protect the rights of Data Subjects for which personal or identifying information is stored. A specific right of a Data Subject is to be able to request and obtain all the information that a Data Controller is holding about them.

A print management system, such as PaperCut NG or MF, stores information about each user including name, email addresses, and printing history.

Print Policy Example:

PaperCut NG and MF now provide a simple tool for reporting all related information for a specific user, making it simple for organizations to meet their data access right obligations.

This feature will export all known information about a specific user that is currently being stored in Papercut NG or MF, including things such as username, print behaviour and history, print job names etc.

5. Support a Data Subject's Right to be Forgotten

Another right specifically granted to Data Subjects is to be able to request that an organization "forget" all information held about them if no longer needed. A typical example is an ex-employee who does not want an organization to retain her printing history.

Print Policy Example:

PaperCut NG and MF now provide a simple command for erasing all identifying information relating to a specific user from the database.

This command deletes the user's account in PaperCut NG or MF, and redacts identifying data including the user's transaction history, job history, account details, and personal details. However, the transactional detail will still be held in the database for reporting and costing purposes, just without any associated user information, e.g. username.

Summary

The GDPR puts obligations on all organizations to take data privacy seriously and protect the rights of their users. This responsibility extends across the spectrum of IT systems, including the print system. At PaperCut we are committed to help our customers meet their GDPR obligations and our solutions provide a range of specific features that help our customers comply.