Think Before You Print: GDPR & Printing

For many companies and private individuals, the hot topic of the year — at least through May 2018 — was the EU General Data Protection Regulation (GDPR for short). After a long period of warnings to prepare, many companies found themselves in a state of chaos trying to implement measures for compliance. Most of the focus was on stolen credit card data or e-mail marketing without the consent of the recipients. But even today, few people appreciate the fact that GDPR also has an impact on document processing and printing processes.

Print jobs are waiting in the queue, while older prints already sit in the printer output tray. Document after document containing personal data which, in order to comply with GDPR, really should be protected. It's a big business risk, because every day documents such as pay stubs, address labels, performance reviews and many other printed documents run the risk of ending up in the wrong hands.

The Consequences of Print

Physical printouts are not the only risk. Today's printers are modern, compact computers that can be hacked. Therefore, data transmission from the end user device to the printer, usually done without encryption, represents a potential GDPR violation.

"Protecting the confidentiality of the personal data stored in the printers is a vital part of a GDPR compliant privacy and data security strategy. Regulatory noncompliance and compromises of personal data can result not only in fines, but, in serious cases, the shutdown of IT operations by the data protection authority," says lawyer Martin Schiefer of the law firm Schiefer Rechtsanwälte GmbH. He further explains, "it is also part of this strategy to delete all data stored on the printers at the end of the life cycle."

Data streams and fitting solutions

As always, the challenge is to get to the root of the problem. Print job encryption must occur on the device where it originates, not during the data transmission or printing process. Encrypted networks offer some relief when it comes to the problem of protecting unencrypted 'data in motion.' Pull printing solutions, on the other hand, address the problem of careless employees. This applies not only to the central office environment and local computer users, but in each branch office and for all devices used for professional purposes. For example, imagine an employee visits a branch and releases print jobs from a tablet. He needs these documents for his next meeting, but they happen to contain highly sensitive data. This scenario can compromise data security. Through the use of pull printing, the print job is available for release at any device, but is only printed after the user authenticates via PIN or with a badge.

This solution is not only practical, but it also ensures GDPR compliance. "In every company today, mobile devices including smartphones and tablets are being used. Pull printing solutions allow these devices to be fully integrated into enterprise-wide printing processes and to meet all GDPR requirements," explains Karin Bopp from Levi, Ray & Shoup, Inc., an expert in output management. The company advises and supports its customers with GDPR-compliant printing solutions. Karin is convinced that it is high time to check existing processes for safety risks and to eliminate those risks, if not done so already.

> ***"Protecting the confidentiality of the personal data stored in the printers is a vital part of a GDPR compliant privacy and data security strategy. Regulatory noncompliance and compromises of personal data can result not only in fines, but, in serious cases, the shutdown of IT operations by the data protection authority."***
> ***Martin Schiefer, lawyer, Schiefer Rechtsanwälte GmbH***

Text translated from German version
© Arbeitsgemeinschaft für Datenverarbeitung (ADV)).

www.LRSOutputManagement.com