Compliance guide GDPR

What are the consequences on print management systems?

About GDPR

Regulation no. 2016/679, known as the **G**eneral **D**ata **P**rotection **R**egulation (GDPR), is the new European reference text on the protection of personal data. It strengthens and unifies data protection for individuals in the European Union. It is scheduled to come into effect on May 25, 2018.
Any breach of the obligations regarding the protection of personal data can be sanctioned by heavy fines.

The **G**eneral **D**ata **P**rotection **R**egulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union.
This regulation applies to any organisation with employees living in the EU, which could collect and process personal information about its employees. The GRDP also deals with the export of personal data outside the EU.
GDPR mainly aims at giving control of their personal data to citizens and residents and to simplify the regulatory environment for international affairs by unifying regulation in the EU.
The **G**eneral **D**ata **P**rotection **R**egulation (GDPR) purpose is to restore control of the personal data of each individual, while improving protection of personal data by applying a set of standardized rules.

To comply with GDPR regulations, organisations must ensure that their IT systems are secure. Organisations must respect the rights of the people concerned and ensure that they give their consent to the storage of information. People concerned should also be able to access their information on request and require their deletion.

Securing the IT system and its design within proper rules are the prerequisites of any compatible GDPR system. The new regulation requires that security must be taken into account from the design and that personal data be anonymised as far as possible.

Why do you have to secure the printing system?

GDPR requirements also apply to the printing system.
An unsecured printing system is a vulnerability factor for an organisation. It can be an entry point for an attack by hackers "hackers" and the printed documents themselves represent a risk of data loss. Unprinted documents stored on the MFP hard disk or in the print queue on the server can also cause data loss.

About Gespage

French technology SME with 45 employees located in Fontenay-Sous-Bois since 1974, Cartadis is the publisher of the Gespage software. Our products, respecting the standards, are produced with a constant goal of quality and reliability.

Gespage is a software solution for governments, companies and the world of education. The "Gespage" Software is dedicated to the management of prints and copies.

This solution enables a print policy to be implemented. It features meter reading, secure printing, redirection rules, statistical reporting and payment management.

Gespage Print Management Software can help you to comply with the requirements of the **G**eneral **D**ata **P**rotection **R**egulation (GDPR).

On GESPAGE, compliance with the GDPR depends on the proactivity of the organisation:

- By securing the network and print servers.
- By securing the print release by the user on all machines (by card or keyboard login).
- By setting access rules to secure printed documents.
- By respecting the right of users to access their personal data.
- By respecting the right to oblivion of users about their printing history.

All the following features are available on Gespage:

- Print management is secure. Securing the print system requires end-to-end security of the print flow (from the time the user sends a print job till the document printing at the point of print).
- Authentication and "pull printing" release (Print2me) avoid "orphan" printings and thus the loss of printed documents. Documents are printed only when the user comes to the printer and authenticates.
- The automatic purge of print "spools" unprinted also avoids lost data.
- Print "spools" remain pending on the print server and are not recorded on the hard disk of the multifunction.
- The information of the users is available immediately by exporting data. A person can easily request and obtain access to all of his information.
- An anonymizing functionality for document titles or user names can be set.
- The information of a user is automatically deleted (directory synchronization) when leaving the structure. Only the print history remains saved for statistics calculation.
- A parameter is also added in the Gespage administration to automatically request the anonymization of print jobs when a user leaves the organization. People therefore have a right to oblivion for their own information.

In conclusion:

The **G**eneral **D**ata **P**rotection **R**egulation (GDPR) requires organisations to take into account the confidentiality of personal data and protect users' rights. This responsibility covers the whole IT system, including the printing system.

Gespage offers all the necessary features that enable client organisations to comply with the **G**eneral **D**ata **P**rotection **R**egulation (GDPR).