uniFLOW

RESPOND
TO GDPR

Secure your print and scan environment

www.uniflow.global

Index

1. What is the European General Data Protection Regulation?

The General Data Protection Regulation (GDPR) is strengthening and unifying data protection for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU. The regulation is in force since the 25th of May 2018 and advocates fines for non-compliance of up to 4% of an organization's annual global turnover or € 20 Million, whichever is higher. Now is the time to ensure your organization is GDPR compliant.

Do you have confidence in your print & scan environment?

- Which documents contain personal data?
- How are documents moved within the company?
- Which systems are involved?
- What steps have already been taken to protect personal data?

2. Complying with rights of the data subject

2.1. Fulfilling a data subject's right of access

The right of access means an administrator is obliged to provide information regardless of whether personal data about the person requesting it is stored or not. If data is stored, a copy of the personal data must be provided upon request.* This also applies to personal data stored for use in an organization's print environment e.g. the user name, email addresses and related print statistics. To comply with this regulation, an administrator must be able to generate a report in a commonly used electronic form.

How can uniFLOW help?

When a user submits a right to access request, an administrator can simply run off a report via a command line to access any user data stored in uniFLOW. All user data from the database is automatically compiled together in a XML file - the file's format must be machine readable by law - which can then be provided to the user.*

2.2. Fulfilling a data subject's right to be forgotten

GDPR grants the right to request personal data be erased, often also referred to as the "Right to Erasure", which must be complied with straight away.* This also applies to personal data stored for use in a print environment. For example, when an employee leaves a company, and requests for his/her data to be deleted from the system, the personal data is no longer required so an administrator must be able to erase the data from the print environment.

How can uniFLOW help?

uniFLOW now includes a command line with which personal data can be deleted from the database. The user's print job history will however remain in the database; it does not contain any personal information so is retained for analytical and statistical reasons which are in an organization's interest. The print job history Is required to verify the overall print volume and the related costs for the financial year. The script also runs a check on the user data to prove to the user that the 'Right to be forgotten' has been conducted properly.

* http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf Article 15

3. Potential risk areas

3.1. Data protection by design and by default

Data protection needs to be integrated into business processes by default to ensure personal data is not accessible to unauthorized parties.[1] How does that relate to printing? When a print job is sent for release, the printed document waits on an output tray until it is collected. In the interim that document, which probably could include personal data, is available to third parties. Employees unintentionally picking up a colleague's document is not unusual i.e., there is a high risk of a breach of personal data.

How can uniFLOW help?

Focus on security:
uniFLOW includes award-winning secure print features. Once installed the security features are activated by default and there is an option to moderate security features where they are not necessary. Print devices can be locked to prevent unauthorized access via access control lists. Scan options can produce encrypted PDFs with optional password-protection. Mobile security is enhanced by providing external job submission pathways which removes the need to add unknown or unauthorized mobile devices to the organizational network.

Safeguard personal print jobs:
The secure printing functionality allows all users to send confidential documents to network printers from desktops or mobile devices. The print job will only be printed once a user has followed the authentication steps while they are physically standing at the device i.e., print jobs are no longer waiting in output trays so they cannot be picked up by a third party. However, when a user's print job is interrupted because the device runs out of paper or into errors, the user might log out without resolving the issue. Whoever logs in next might be able to resolve the issue and receives the print job of the previous user. uniFLOW prevents this case by automatically deleting the pending print job upon a user logging out.

3.2. Security of Processing – Reduce risks

To ensure the security when processing personal data, GDPR requires implementation of technical and organizational measures which are appropriate to the risk involved. The print and scan environment faces the following challenges: secure transfer and storage of personal data, resilience of the system and the ability to restore personal data in a timely manner following a physical or technical incident.

How can uniFLOW help?

uniFLOW secures end-to-end connection between devices by encrypting print jobs in transit using AES-256-bit encryption. To ensure continuous availability of the print and scan infrastructure uniFLOW offers various options. A three-pillar model consisting of an automatic Canon MEAP device failover, redundant spool file storage and intelligent print job distribution create a holistic resilience solution. Server backups mean personal data can be retrieved in a timely manner, as required under GDPR, and facilitate smoother processing of business workflows. When registering a user to uniFLOW only a minimum of data is asked for to avoid the storage of redundant personal data.

1 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf Article 25

3.3. Detection and reporting – Limit the damage

Once an administrator is aware of a data breach, GDPR stipulates that it must be reported to the supervising authority within 72 hours. The notification must include details as to the nature of the personal data breach and its likely consequences. This means organizations must develop a strategy regarding how to react if a data breach occurs and review their auditing procedures. Up to a quarter of data breaches are paper based, so it is crucial your print software can track the cause of a data breach.[1]

How can uniFLOW help?

Under GDPR, investigations into data breaches will be mandatory. Integration between uniFLOW and Canon's iW SAM Express means text and image data can be captured together with log information to facilitate in-depth auditing and flagging of confidential information for a review. All data and images can be exported to a Data Loss Prevention System. Furthermore, iW SAM can accelerate detection of data breaches by notifying a designated administrator e.g., when a specific keyword is printed. After a data breach happened the administrator can quickly track and report which documents has been printed, copied, or faxed and by whom.

1 http://www.computerweekly.com/news/1280095740/Infosec-2011-Canon-highlights-security-risk-of-improperly-configured-printers

4. FAQ

Is an ISO 27001 certified organization GDPR compliant?

ISO 27001 does provide a framework for data protection and offers guidelines as to how to instigate measures for data protection. However, contrary to what some internet articles suggest, ISO 27001 does NOT serve as proof of GDPR compliancy. Neither does it certify any software products. In conclusion, compliance with GDPR is more than simply a case of collecting certificates; it requires an intensive analysis of processes and software currently in use.

When using uniFLOW - Who is the data processor and who is the data controller?

When installing uniFLOW, security settings are activated by default. By providing GDPR related tools (e.g., for the Right to Access and the Right to be Forgotten) and a set of security features uniFLOW will facilitate GDPR compliancy for any organization. However, an administrator might decide to reduce security settings, choose an insecure server or carry out modifications – actions that cannot be controlled by NT-ware. All responsibilities of the data processor and data controller lie with the organization using uniFLOW.

Will more GDPR related features be added to uniFLOW?

uniFLOW is constantly further developed and always has security at the forefront. Regular QA testing and identified security threats are analyzed as a high priority to ascertain the threat and resolve it. Review and development of uniFLOW also includes new features to facilitate an organization's duty to meet GDPR requirements.

Where can I receive more technical details about uniFLOW?

Canon and authorized resellers can explain more technical details and answer additional questions. Where weak spots within the current print environment have been detected, Canon and authorized resellers can help to eliminate these. This document is a NT-ware marketing document only with the aim of informing customers how uniFLOW can help organizations comply with the new GDPR regulation. It does not replace an organization's obligation to inform themselves about all necessary steps to become GDPR compliant

www.**uniflow**.global
www.**uniflowonline**.com