RESPOND TO GDPR

SECURE YOUR PRINT AND SCAN ENVIRONMENT

WHAT IS THE EUROPEAN GENERAL DATA PROTECTION REGULATION?

The General Data Protection Regulation (GDPR) will strengthen and unify data protection for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU. The regulation will come into force on 25th 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; 91% of businesses have already incorporated security measures into their printing practices or are planning to do so.*

*http://quocirca.com/content/managed-print-services-landscape-2017

DO YOU HAVE CONFIDENCE IN YOUR PRINT & SCAN ENVIRONMENT?

"GDPR also affects UK businesses. The re-gulation becomes law on 25th May 2018, before the UK leaves the EU, and the Government has confirmed the regulation will remain afterwards."*

An organization will be well informed if the internal and exter-nal processes are analyzed before deciding which technologies or processes are necessary. When considering the print envi-ronment the following questions should be addressed:

- 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?

*https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf

POTENTIAL RISK AREAS

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.* 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 inclu-de 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 ins-talled the security features are activated by default and there is an option to moderate security features where they are not necessa-ry. 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 pro-viding 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.

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

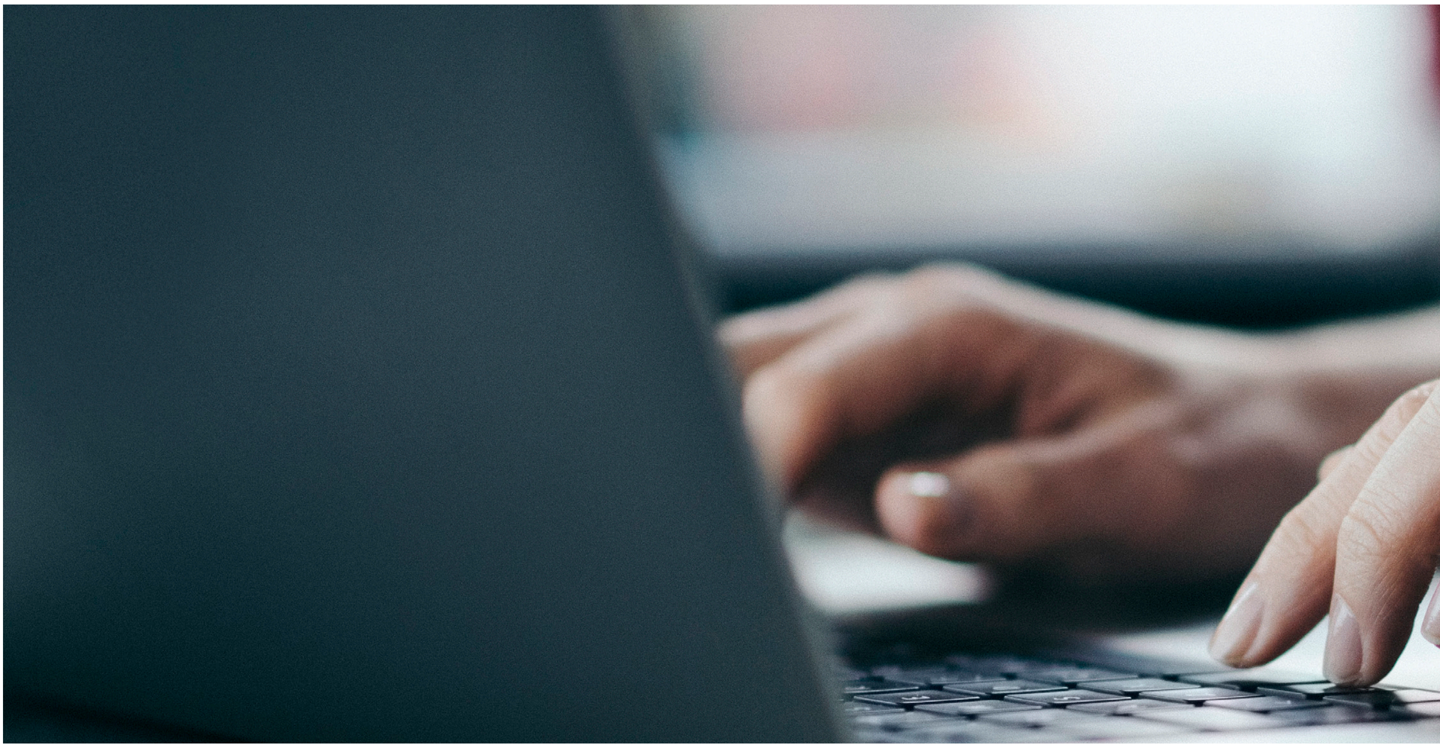
SECURITY OF PROCESSING – REDUCE RISKS

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 environ-ment 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.

*http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf Article 32(1)

How can uniFLOW help?

uniFLOW secures end-to-end connection between devices by enc-rypting 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.



DETECTION AND REPORTING – LIMIT THE DAMAGE

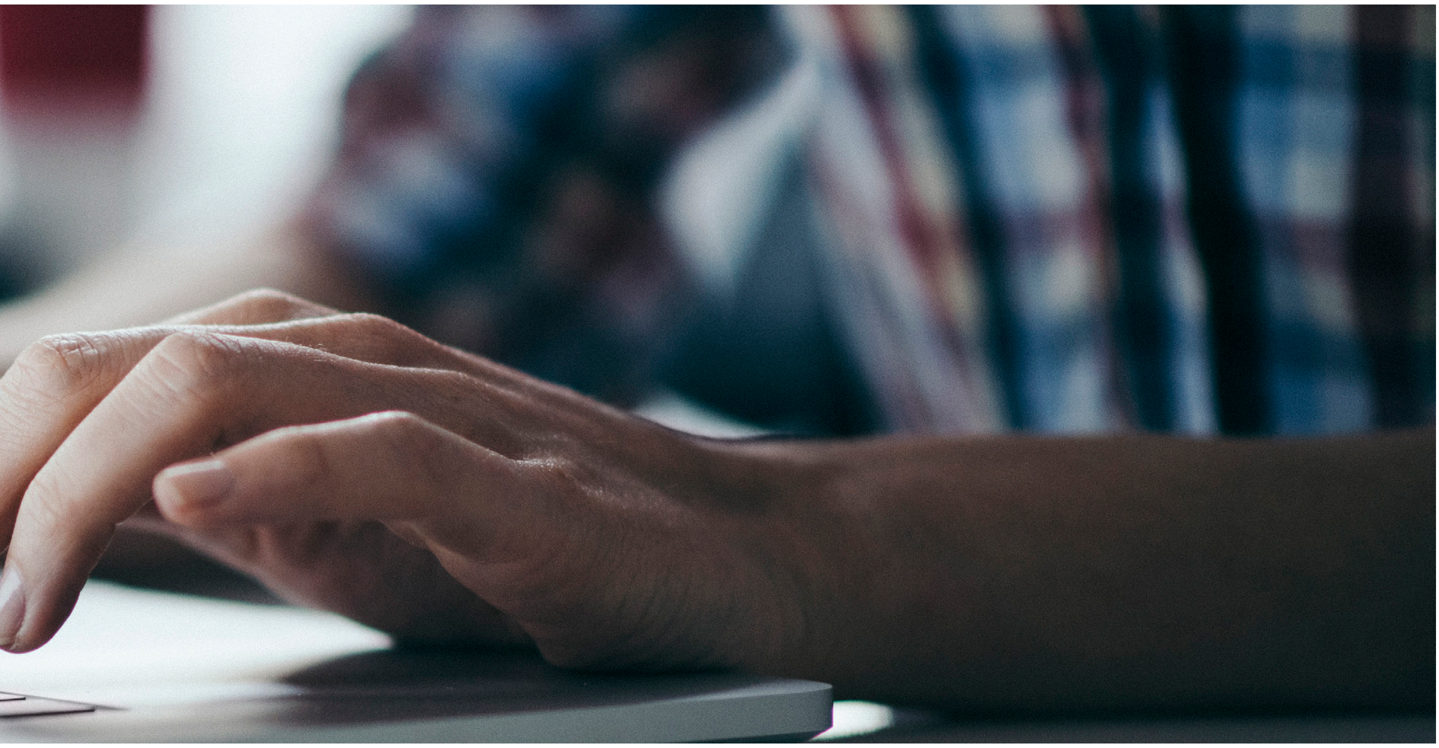
Once an administrator is aware of a data breach, GDPR stipulates that it must be repor-ted to the supervising authority within 72 hours. The notification must include details as to the nature of the personal data breach and its likely consequences. This means organizations must develop a strategy regarding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

> **"Data breaches need to be reported within 72 hours to the national regulator."***

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 Preven-tion System. Furthermore iW SAM can accelerate detection of data breaches by no-tifying 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.

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



FAQ

Is an ISO 27001 certified Organization GDPR compliant?

The ISO 27001 regulation does not serve as proof of GDPR compliancy. However it does provide a frame-work for data protection so ISO 27001 can help an organization to become GDPR compliant. It does not guarantee compliancy. So, in the end, it is an organization's responsibility to choose software which complies with GDPR.

Does NT-ware fulfill ISO 27001 Regulation?

Organizations who wish to comply with ISO 27001 must apply for certification and complete a formal com-pliance audit. Currently NT-ware has not applied for ISO 27001 certification.

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 requi-rements.

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.

CANON NORGE AS

Postadresse:
Postboks 33, Holmlia, 1201 Oslo

Besøks- og leveringsadresse:
Hallagerbakken 110, 1256 Oslo

Tel: +47 22 62 92 00
Faks: +47 22 62 92 01

www.canon.no

Version 1 | November 2017