How to keep printing, scanning & copying processes GDPR compliant.

xenith
document systems

WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR?)

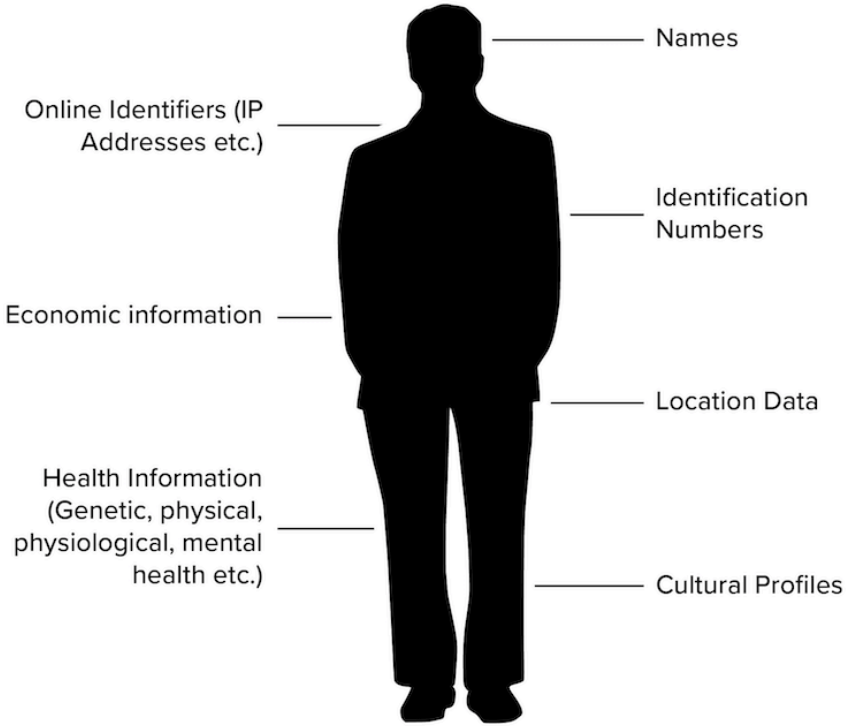
The General Data Protection Regulation (GDPR) is set to replace the Data Protection Act 1998 (DPA) and will come into effect from the 25th May 2018.

It will regulate the processing and holding of personal data.

While similar to it's predecessor, GDPR has some key differences in terms of personal data classification and scope, accountability and compliance, breach notification procedures and penalties.

PERSONAL DATA CLASSIFICATION AND SCOPE

The type of data protected has vastly increased and includes economic, cultural, usernames, pseudonyms, online footprint information, etc. For example, under GDPR, IP addresses are classified as personal data.



ACCOUNTABILITY AND COMPLIANCE

“The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.”

[Information Commissioner’s Office]

BREACH NOTIFICATION PROCEDURE

New breach notification procedures are required - and there's a 72 hr time limit for reporting a breach.

"You should ensure that you have an internal breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public. In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place."

[Information Commissioner's Office]

PENALTIES

The penalties being introduced with GDPR could be enough to put some organisations out of business.

With penalties amounting to as much as €20 million or 4% of global annual turnover (whichever is greater), it's worrying to think that all of this can be the result of a poorly protected print/scan/copy process.

In order to remain compliant with the GDPR, you need to implement measures to:

Protect sensitive information within documents

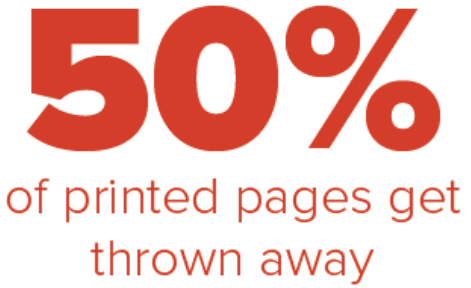
Prevent sensitive data from being shared inadvertently

Have robust processes to detect possible breaches quickly

Have documented processes

WHY IS PRINT SECURITY AN ISSUE? (AND HOW WILL IT AFFECT GDPR COMPLIANCE?)

Initially, it may not be clear how document and print security might affect GDPR compliance, but when you consider that around 50% of printed pages get thrown away [Xerox], what if your employees are putting sensitive data straight in the bin?



As much as sixty-two percent of data breaches are down to human error [Computer Weekly]. Think of the stories you hear when people leave sensitive data on the train or in a cafe, it's potentially easily done when people aren't aware of what personal data is and such cases could be liable for penalties under GDPR.

62%

of data breaches are down to human error

Organisations need to be able to protect sensitive information within documents and prevent sensitive data from being printed and shared inadvertently. This will mean having robust processes to detect possible breaches quickly and documenting processes, whether that be preventing a document from being printed or alerting someone to what's happened.

HOW TO SECURE YOUR PRINTING PROCESSES

BASIC SECURITY MEASURES

Here's what we recommend you put in place as basic security measures. In most cases, these features come a standard with Xenith's MPS Plus:

Cisco Trustsec
Helps identify, monitor and manage devices from a central location. Real-time views and control over all users and devices on a network.

McAfee Secure Device Whitelisting
Allows only approved files to run on MFDs, offering significantly more protection than traditional black listing tactics.

Encryption
Ensures that data travelling between devices is kept secure.

Image Overwrite
Electronically shreds copy, print, scan & fax jobs stored on the MFD's hard disc.

Follow-me printing
Releasing documents only on authentication with your door entry card/ mobile/PIN code at the device prevents them getting into the wrong hands.

5 WAYS TO REDUCE DOCUMENT INFORMATION RISK

1) A user-centric view of document output and input

2) Monitor who prints document information within the business

3) Monitor security across document lifecycles

4) Check the vulnerability of your endpoints

5) Keep document information safe

PRINT AND DOCUMENT SECURITY EDUCATION

Educate everyone on the risks of printing sensitive data and what counts as sensitive data, because at the end of the day, if someone doesn't know it's wrong, why would they stop?

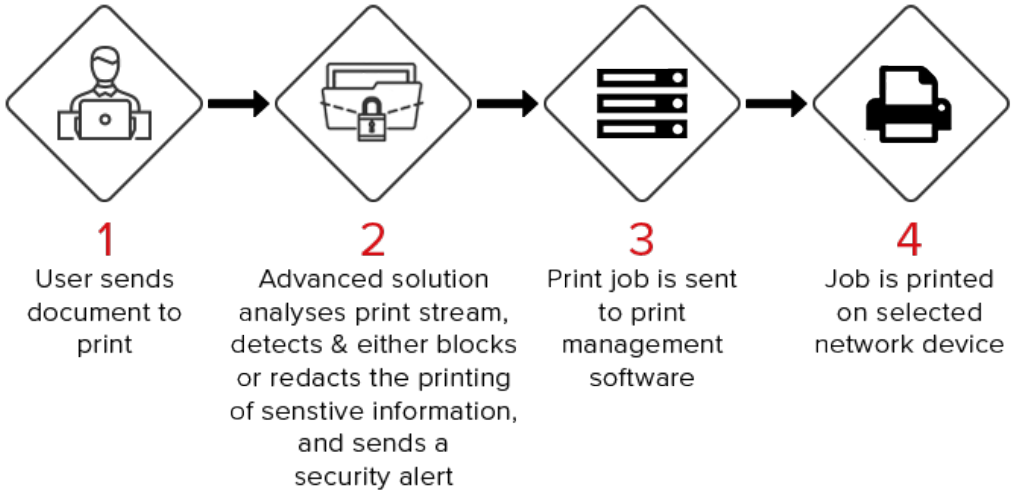
To educate employees, you might choose to send an internal email or use an in-house communication channel. If you choose this method, make sure you have some resources that make it easily accessible and understandable, either an internal document you can share or something official.

ADVANCED SECURITY MEASURES

With advanced security measures, print/scan/copy streams can be automatically scanned to detect and block/redact the release of any sensitive data from the device.

It’s even possible to redact sensitive data from the document being printed/copied/scanned without affecting the master document, or without the need for any manual intervention.

On top of this, overlays like security stamps can be added as a rule when sensitive data is detected in a document, or alternative workflows can be triggered in order to send the document to a secure location for review before permission is granted to print it / copy it / release the scanned file.



HOW TO KEEP PRINTING & DOCUMENT PROCESSES GDPR COMPLIANT

With GDPR coming into effect on the 25th May 2018, it's important to start acting now in order to remain compliant and have all procedures in place.

Here's what you need to do:

- Protect sensitive information held in digital format, and prevent access to it by unauthorised individuals.
- Prevent sensitive data from being printed.
- Detect possible breaches quickly and easily, in case they take place despite best efforts.
- Ensure documented processes are in place to illustrate compliance and accountability.

ADDITIONS: XENITH'S ADVANCED SECURITY PACKAGE

- Automatically analyse print, scan and copy streams to detect sensitive data
- Redact sensitive data before it's printed
- Block documents from being printed entirely
- Trigger workflows to get approval for printing
- Trigger workflows to add security stamps/barcodes
- Alert the security officer of a scanned or printed document

All done behind the scenes, without affecting the master document.

Contact us about our advanced security package.

A Short Guide:
How to keep printing, scanning & copying processes GDPR Compliant

Our new guide explains:

- How GDPR affects printing/copying/scanning
- How to secure your printing/scanning/copying processes
- How to automatically analyse print, scan and copy streams to detect sensitive data that can be redacted or blocked or trigger security alerts

DOWNLOAD A COPY