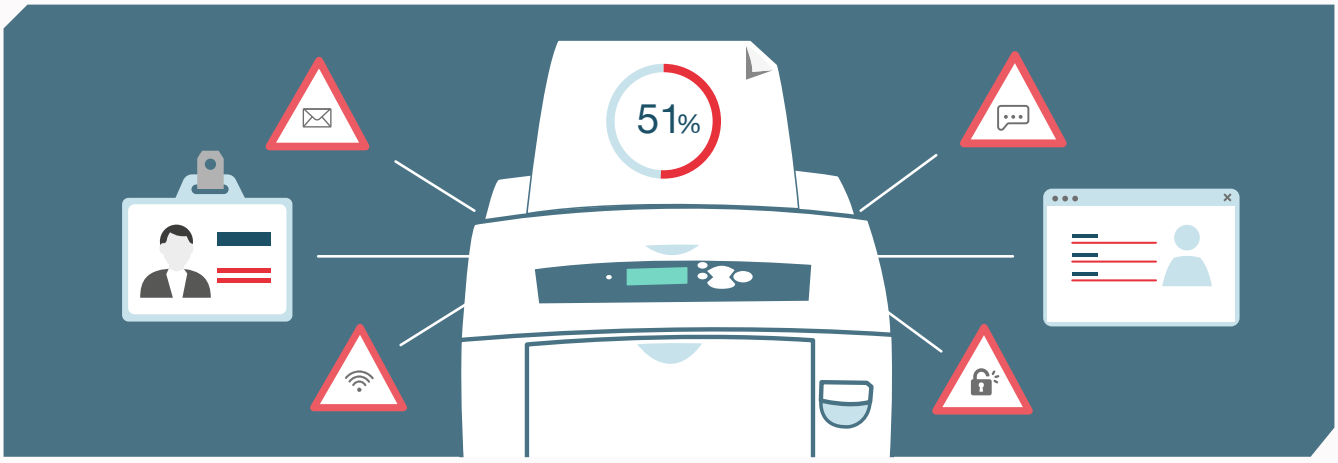
PRINT – THE MISSING LINK IN YOUR GDPR STRATEGY

As of 25th May 2018 the biggest changes to data protection law in recent history will come into force – The General Data Protection Regulation. If you've been paying attention to the hype, you'll know it's not a matter to be taken lightly. The regulation will affect any organisation that stores or processes the personal data of EU citizens, and failure to comply with the regulation could see businesses face fines of up to €20 million or 4 per cent of their global turnover[1] (not an insignificant sum). Whilst organisations across the UK are scrambling to shore up their data storage and security policies in time, many are overlooking a critical aspect of their business that could be leaving them vulnerable – their print environment.



According to an IDC survey of print and imaging decision makers, 51% of respondents mistakenly believed the GDPR excludes printing.[2] Even now you're probably thinking that your printers are the least of your worries when it comes to the GDPR. Well, you might be surprised just how wrong that assertion is.

1. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1
2. Western European Hardcopy Survey, IDC, Q2, 2017

What's It All About?

You'll be forgiven for not having trawled your way through the EU's lengthy documentation on the regulation, but there are a few significant points you should be aware of. Article 5 of the GDPR outlines the six principles that should be applied to any collection or processing of personal data. Most notably point F states that,

> *Personal data shall be… processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')* [3]

You're probably wondering how this affects your print environment. Print devices process and store vast amounts of personal and often sensitive data, with employees across your organisation making use of them on a daily basis. The EU defines personal data as, "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address."[4]

It's easy to see how any one of these examples could find its way onto a print device. For instance, your HR department might be printing an employee's contract one minute whilst your finance department scans an invoice the next. On top of all of this,

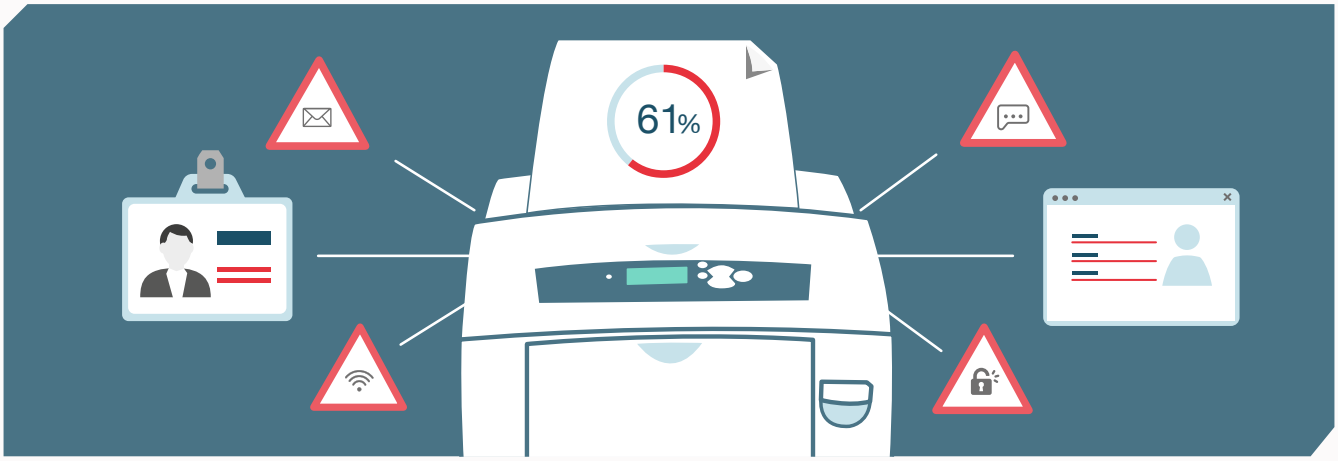
> *The GDPR requires you to show how you comply with the principles – for example by documenting the decision you take about a processing activity.*[5]

This ranges from providing comprehensive, clear and transparent privacy policies to keeping records of all processing activities.[6]

3. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1
4. http://europa.eu/rapid/press-release_IP-12-46_en.htm
5. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/
6. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/

Why Is This A Problem?

Print environments are notoriously overlooked by security teams despite being liable to a number of insider and outsider threats. According to a recent survey by Quocirca, 61% of large enterprises have admitted suffering at least one data breach due to insecure printing.[7] As printers are essentially Internet of Things devices, they're a potential door to your entire corporate network. If they're left unsecured, it becomes all too easy for unauthorised users to connect, especially as mobile printing becomes an increasingly popular option.



Even if your defences prevent access to your network via your print devices, a huge amount of sensitive information is processed and stored by them. This means that access to the device itself could lead to a data leak. On top of this, human error and a lack of secure print measures can even lead to confidential documents being printed and left on devices. In these instances unauthorised employees can end up stumbling across information they should not be seeing – something you probably want to avoid regardless of the GDPR.

As you need to document how you're complying with the GDPR, you might run into trouble if a) you can't demonstrate that your security systems are effectively preventing mismanagement of your data, and b) you're not recording all of the traffic that passes through your print devices. This becomes even more problematic when you consider the fact that GDPR compliance is probably the last thing going through your employees' minds when they're heading to the printer.

7. http://quocirca.com/content/print-security-imperative-iot-era

What Can You Do About It?

Fortunately, there are number of intelligent print management solutions on the market that can provide you with extensive control of your print environment. As well as allowing you to monitor all usage of your print network, they include proactive measures that can prevent unauthorised access. Essentially they're one of the most effective ways to ensure that no personal information goes awry, whilst providing you with a host of other benefits.

Firstly, a managed print services provider will perform an assessment of your organisation's current print environment to identify any vulnerabilities or gaps in your security. Chances are you've missed something.

This can then be utilised as part of a Data Protection Impact Assessment (DPIA), which many organisations will be required to undertake by the GDPR.[8]

Amongst other functions, management solutions can enable IT administrators to set up automated workflows. These can detect if documents contain specific patterns relating to sensitive data (like NI numbers, bank/credit card details, personal health information or sensitive company data). It can then redact all instances of that pattern in a document. Xeretec's secure print and scanning solution, powered by Nuance Output Manager and integrated with a Follow-You solution, is even sophisticated enough to flag up incidents of potential compliance violations to a company's Chief Data Officer, Security Manager or Head of Compliance, thereby acting as an early warning system ahead of a potential breach.

Thanks to managed print solutions, the GDPR doesn't have to mean an end to mobile access to print devices. They can provide administrators with the power to track and control access to all print devices within their network, ensuring any and all unauthorised access is flagged and blocked before a breach can occur. Alternatively they can provide the option to hold documents securely at the printer until the user logs in at its interface and selects print. This will also help you meet your documentation requirements, as you can keep records of each individual use.

Another potential option is to whitelist known designated users, specific IP addresses or predefined types of services to pass through your system, allowing companies to set up rules over which traffic is allowed to pass through rather than having to accept each print request manually. In this case all whitelisting authorisation would run through the administrator and not the user – the last thing you want is users clicking approve on every popup they receive.

8. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1

Meanwhile, other solutions can provide companies with a secure print function. This allows only those with the correct authorisation to release prints from a device via a secure PIN code or swipe card. This is a highly effective way to stop unclaimed documents being left on devices and accessed by the wrong people – whether that means ill-intentioned intruders or simply distracted employees.

Conclusion

Whilst there's not long to go until the GDPR kicks in, getting your organisation in shape doesn't have to be the struggle that many are making it. By partnering with a managed print service provider you can guarantee that all of your print processes are GDPR compliant, whilst simultaneously closing up a gaping hole in your organisation's defences.

The Xeretec Group is a leading integrator of digital print hardware, software, solutions and services, supporting the print needs of businesses across the UK, Ireland and Western Europe. Established in 1991, Xeretec has grown to become Xerox's largest partner in Europe. The Xeretec Group also includes the Landscape Group - the UK's most accredited HP MPS and Solutions Specialist - which was acquired by Xeretec in June 2017.