



Are your business's print and scanning security functions ready for the most important change in data privacy regulation in two decades?

Anthony Buxton, Senior Manager, Legal & Corporate Governance at Brother International Europe, comments on device security as the implementation of European General Data Protection Regulation (GDPR) draws ever nearer.

Information security was already on the radar of SMBs across Europe according to research conducted just two years ago, with 75%¹ admitting it was important to their organisation and 59% saying it impacted on decisions around printing and document management.

Meanwhile, a new study of European mid-market businesses and large enterprises conducted this year has revealed that 96%² view print security as important. But despite this acknowledgement, there's a distinct lack of confidence among companies. Only 22% of European enterprises indicated they are completely assured that their print infrastructure is protected from threats.

The data also revealed that larger organisations are ahead on GDPR and print security. Large organisations (53%) are more likely to include print security within GDPR measures, more than double the percentage of mid-market organisations (24%).

Turning back to SMBs, and with the enforcement of [European General Data Protection Regulation \(GDPR\)](#) just months away, how can small and medium sized businesses look to protect their print operation from data breaches?

The potential penalties for non-compliance are huge with maximum fines of €20 million euros or 4% of global turnover (whichever is greater). Fines aside, there is a growing customer expectation of compliance as individuals become more aware of their personal data rights. SMBs' reputations now depend on good data practice and as part of that they need to take their print and scanning practice seriously.



Having the threats in your field of view

Printing and scanning set-ups are becoming increasingly versatile and powerful. Increased functionality and connectivity comes with additional security risks for networked devices.

Four key areas of risk include:

- 1) Accidental leaks of confidential print-outs
- 2) Accidental leaks of confidential scans
- 3) Network intrusions due to inadequate security
- 4) Unauthorised users gaining physical access to unguarded devices

In short, if someone can collect your documents from a printer and walk away with them, data is at risk and your business could be liable.

For the SMB, protection against a breach in your business's print and scan functions doesn't automatically mean a large outlay or an upgrade to new equipment to meet the requirements of the new landmark legislation.

Our printing and scanning devices have a host of embedded security features that can be deployed to 'serve and protect' a business from GDPR's heavyweight penalties.

Our security solutions are ideal for business sectors including HR, finance, healthcare, retail, legal and education, but are equally applicable across all landscapes where data confidentiality is crucial.

Secure Print

Ideal for small businesses that occasionally need to print confidential documents, Secure Print is free and built in to many of our devices. When printing a sensitive document, users can select the Secure Print function and will be asked for a four-digit code. This needs to be inputted into the machine to release the document, delaying the print until the user is physically in front of the device – ideal for a printing device with multiple users.

Secure Print +

Aimed at SMBs with greater security requirements, users are given an ID card to swipe to release their print. This works through Near Field Communication (NFC) and is linked to a unique employee number. The card creates ease of use as employees don't need to remember a pin code to release print jobs.

Secure Print can be used to control scanning, copying and faxing function and allows a device to be configured to automatically delete print jobs if uncollected.

Secure Function Lock

This free functionality allows a business to have more control over their devices, restricting access to the machine's settings through its control panel. Secure Function Lock also restricts access to certain functions, which allows businesses to decide which employees can do what with a device. That could range from the ability to control who can print, scan, copy or fax or impose monthly limits through PIN numbers and NFC cards.



With GDPR fast coming into sight on the horizon, deploying these settings can significantly reduce the risk of unauthorised access to sensitive data. Without the lock functionality, the scan to email setting could be changed for example, resulting in an unapproved email address receiving confidential information.

PrintSmart SecurePro

A more advanced security solution aimed at SMBs and larger enterprises, PrintSmart SecurePro provides complex print device protection for businesses where the need to print confidential documents varies for different users. As a server-based solution, PrintSmart SecurePro is therefore ideal as it doesn't use up memory on a device.

Its 'pull printing' feature which releases a document through a pin code or an ID card on an NFC reader – protects sensitive documents plus any job that doesn't get 'pulled' is deleted after a set length of time. This eliminates the risk of a confidential document being obtained by an unauthorised employee.

So, only the user who sent the print job can collect it, which means confidential data will only be viewed by an authenticated user.

If a data leakage did occur, PrintSmart SecurePro provides a robust audit trail. The report can be swiftly generated and can include details of time, date, IP address, page count, A3 or A4 paper and mono or colour print. This high level of detail makes investigation into the print activity easier to review, in line with GDPR requirements.



Encryption embedded

Occasionally with certain software, businesses should be aware that data can be intercepted as it travels to the printer itself. To safeguard against this, our devices have embedded Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption. This is the same technology used in e-commerce to protect bank and credit card details. So your most confidential files can be encrypted at up to 256-bit during transmission over the network.

Our suite of solutions help address print and scan security for the SOHO with little or no IT infrastructure, to SMBs or larger enterprises in preparation for GDPR enforcement on 25th May 2018.

Size of business is no excuse and time is ticking.

¹ Brother SMB Research conducted in 2015 by B2B International among 2,502 businesses in the UK, France, Germany and USA.

² Quocirca Managed Print Services Landscape, 2017. European survey results of 180 midmarket (500-999 employees) and large (1000+ employees) organisations in UK, France and Germany using a managed print service.