Information Security White Paper

GDPR Compliance

An introduction to Information Security

Contents

SHARP

Introduction

All modern businesses face challenges trying to ensure compliance with the EU General Data Protection Regulation (GDPR), especially when it comes to personal data protection.

The General Data Protection Regulation (GDPR), has brought several challenges to businesses across Europe and globally.

While a lot of focus of the GDPR is on protecting online data, it also applies to how businesses work with and store the data, which means that they need to consider what happens to the information that they capture (through scanning or electronic input), store and retain, process, share, print, copy, fax and archive.

The regulation introduces categories such as Personal identifiable data, Data protection, Data erasure, Data Processors, Data Controllers, Data Protection Officers, Compliance, Data Protection Authority and more (see the GDPR Glossary on pg.6).

There are many publications focusing on how to interpret the GDPR wording, who will be affected and how to introduce this regulation into businesses. However, there are only a small number of documents, articles or white papers on how to translate GDPR into real business language and all of the processes linked to the business activities, especially those associated with personal data.

By linking business users (employees), business processes (workflows and best practices) and business assets (hardware and software), Sharp has defined three separated areas of business security that, when brought together, can enhance overall business security to deliver GDPR compliance.

These three areas are:

1. Network Security

Relating to any network used by a business organisation, maintained by an IT department, where emphasis is put on all connected printing, scanning and faxing peripherals.

2. Output Security

Relating to both the printed and scanned output from MFPs or Printers. This category includes hard copy printed documents and images of documents in transit from a PC to a printing device (including through dedicated print servers), scan (including scan-to-folder, scan-to-email, scan-to-cloud) and fax.

3. Document Security

Relating to information captured from paper documents through the scanning process or electronic images of the documents stored in business repositories, e.g. emails, electronic files, forms, etc.

Sharp can help businesses achieve GDPR compliance by introducing and applying a set of tools and best practices to business processes, linked directly to Network, Output and Document Security.

Background

GDPR is the biggest change to happen to data protection in more than 20 years. But there are still many questions – and limited answers.

> GDPR introduces new requirements and defines the financial penalties of not having sufficient guards and preventative measures to protect against breaches[1].

But very limited guidance is given on what business owners, IT managers and users need to introduce to be compliant. It is left for each business to interpret what to put in place.

The main point of introducing the GDPR was to better manage and protect the processing of personally identifiable data. That means all personal information in your business systems – from customer and business contact data stored in business applications, through all network settings, document management and print management accounts, to HR documentation on staff – should be managed in the appropriate manner.

There are two main layers of the GDPR compliance:

Personal layer
All matters related to the user, including their behaviour, way of working and how business systems and rules are applied to them

Organisational layer
The business processes within an organisation (including paper and electronic workflows), assets (including those that help people share and communicate in an electronic or paper-based way), the culture and how it responds to market challenges.

> By introducing strategies and tools at an organisational level the expected change in behaviour of end users and how they work and process all the available business data can be set and managed. That leads to a better understanding of how to process both documents and user identifiable data.[2]

Therefore, Sharp focuses on the organisational layer (processes, solutions, and hardware) and can help to build comprehensive security policies that are crucial for every business.

Focusing on three areas of business security, Sharp has outlined potential risks that could lead to compliance breaches if not addressed:

Network-related risks

- The vulnerabilities of moving data between paper and electronic formats and back out to paper.
- The need to secure MFPs and Printers to the same level of servers and the necessity of a planned and unified Print Security Policy.
- The need to monitor and manage devices to sustain and update, when necessary, the Security Policy in line with new vulnerabilities over time.
- The need to dispose of data securely and in a timely way.

Output-related risks

- The need to secure the access to MFPs and print devices, to control output and routing of confidential data.
- Managing the number and types of outputs – copies, prints, faxes, scans (including scan-to-email and scan-to-folder).
- The need for an audit trail and accountability for what was captured or printed.

Document-related risks

- Lack of definition and understanding of the document lifecycle in the business. This includes all steps of the document lifecycle, from document creation to document disposition.
- Unstructured document repositories that leave document management systems open to attacks and potential breaches.
- Repetitive manual tasks linked to (electronic and paper) documents, whereby a wrong destination could be added by mistake and lead to data breaches.
- Uncontrolled sharing of business-critical documents.
- Risk of data corruption without version control.

Recommendations

Using our comprehensive approach to business security, Sharp can ensure compliance with the strictest regulations, and create solutions that help businesses work more effectively.

Sharp aims to ensure GDPR compliance in every aspect of information security by addressing the three main areas of business security: Network Security, Output Security and Document Security. We cover the organisational aspects of Data Processing and Data Protection through our comprehensive portfolio of Optimised products and solutions, as well related Sharp Professional Services.

By building a strong base across the organisational layer of a business, we can influence end user behaviour. This, along with our well-designed and secure systems, helps businesses comply with GDPR and delivers the appropriate tools to measure risk, prevent cyber-attacks and deliver accurate user-related insights.

Sharp Professional Services cover every aspect of data security, including how personal identifiable information is handled in business systems, helping organisations comply with GDPR.

The below is a summarised table that shows how Sharp can help you comply with GDPR:

General Data Protection Regulation and Sharp		
Security Aspect/Area	Products and Solutions	Compliance through:
Network Security	Sharp MFPs Sharp Printers Sharp Remote Device Manager	User access control Port control Protocol control Network Services control Data encryption Data overwrite
Output Security	Job Accounting II PaperCut MF SafeQ Drivve Image Prism ScanPath	Access control Functionality restrictions Data log / Audit reporting Data log retention and redaction
Document Security	Cloud Portal Office Drivve DM Docuware Drivve Image Prism ScanPath	Database access control User rights control Version tracking Audit trail Document retention, *incl. document disposal* Audit log

Conclusion

Sharp can help organisations establish effective security measures and effective management methodologies to help achieve GDPR Compliance.

To understand, plan, configure and execute the measures and functions required to be compliant with GDPR could take much time and cause real implementation difficulties, especially as every business is different.

Sharp recommends that business owners and IT managers can access the white papers provided in our library for guidance on the three subject areas of Network Security, Output Security and Document Security:

www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/information-security.htm

These papers will describe the risks and mitigations and introduce:

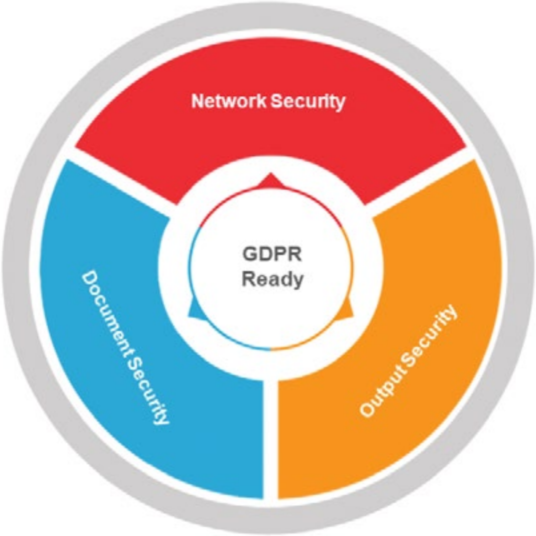
- Sharp secure network devices
- Sharp security software that helps to protect business data capture and output
- Sharp security software that helps to protect electronic documents.

In addition, the Sharp Professional Services teams offer consultancy and help to build robust security measures and introduce tools relevant to each business type and need.

To avoid potential vulnerabilities in other areas of your organisation, we can help you introduce further security measures from the Sharp portfolio, so that you can deliver 360-degree security protection for every aspect of your business:

- Document Security
- Network Security
- Output Security
- GDPR compliance

Sharp Security Framework



GDPR Glossary [3]

Accountability – the data controller is responsible for compliance with the data protection principles. They must be able to demonstrate the steps the business takes to ensure compliance.

Data Breach – any accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access of a subject's data.

Data Controller – 'controller' means the legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data.

Data Erasure– (also known as the Right to be Forgotten) this entitles the data subject to request that the data controller erase their personal.

Data Processor – 'processing' means any operation, or set of operations, which is performed on personal data or on sets of personal data. It is considered processing whether these operations occur by automated or manual means. Processing includes the following activities: collecting, recording, organising, using, structuring, storing, adapting, retrieving, consulting, destroying and more. The data processor can be an organisation or third-party provider who manages and processes personal data on behalf of the controller. Data processors have specific legal obligations, such as maintaining personal records, and are liable in the event of a data breach.

Data Protection Authority – the national authority who protects data privacy.

Data Protection Officer – an appointed individual who works to ensure you implement and comply with the policies and procedures set by GDPR.

Data Subject – someone whose personal data is processed by a controller or processor.

Personal Data – any direct or indirect information relating to an identified person that could be used as a means of identifying them. This includes their name, ID number, location data or an online identifier.

Processing – this refers to any activity relating to personal data, from initial collection through to the final destruction. It includes the organising, altering, consulting, using, disclosing, combining and holding of data, either electronically or manually.

References

1. UK firms could face £122bn in data breach fines in 2018. *ComputerWeekly, October 2016*

2. CEO Survey. *PwC, 2017*

3. GDPR Glossary of Key Terms. *High Speed Training, February 2018*