GDPR Print Compliance Guide

The GDPR overview

One Q has developed this GDPR guide together with Devoteam to help and assist customers getting Print, Copy and Scan processes GDPR compliant. The intention is to help companies getting an overview of their specific situation which triggers the needed security measures relevant for them.

The guide suggests measures, both digital and manual, in order to become regulatory GDPR compliant, and offers argumentation for this in a GDPR context.

To set the scene we have provided two pages of general GDPR information, which you can skip if you are familiar with GDPR.

Disclaimer

1. This guide does not provide legal advice and does not create an attorney client relationship. If you need legal advice, please contact an attorney directly.
2. To obtain GDPR compliance suitable manual and digital procedures and processes around the One Q solution must be established.

What is GDPR

The General Data Protection Regulation, or GDPR, is set to replace EU member states national data protection acts, and will come into effect from May 25th, 2018.

GDPR will regulate the processing and holding of personal data including the free movement of such data, ultimately changing how business and public sector organisations can handle the information of their customers. The regulation applies to both data controllers and data processors, which is handling and storing personal data as a part of their activities in offering goods or services to citizens in European Union and any behavioral monitoring of citizens within the European Union.

The GDPR is designed to “harmonize” data privacy laws across Europe and it provides individuals with greater control over their personal data and assurances that their information is being securely protected. Effectively this is EU’s way of giving individuals, prospects, customers, contractors and employees their rightful power over their data and decreasing organisations power to collect and use personal data without consent.

Compliant with GDPR

The regulation requires that data controllers show accountability and are responsible for demonstrating that they comply with the principles in article 5 (1). Organisations should position themselves to explain how they protect the data they process and store and how they work to remain compliant with the regulation. It is under this consideration that organisations must demonstrate that their processing activities, using printing, scanning and copying for data protected under the GDPR, comply with the regulation.
Hence, organisations generally need to implement measures to:

- Protect sensitive information in systems and documents
- Control access to and sharing of sensitive information
- Detect data breaches and manage communication to stakeholders
- Assign clear roles and responsibility within the organisation
- Document data protection policies and processes

Business implications of GDPR

All organisations and companies working with personal data should appoint a data protection officer or data controller within the company, who is in charge of GDPR compliance.

There are tough penalties for those companies and organisations who don’t comply with GDPR - fines of up to 4% of annual global revenue or 20 million Euros, whichever is greater.

Many people might think that the GDPR is just an IT issue, but that is far from the truth. It has broad-sweeping implications for the whole organisation, including the way companies handle personal data or sales and marketing activities. Printed documents is an essential part of this and companies must have a plan for securing personal data that is being printed.

How to use the guide

Find your organisation’s needs/level moving from left to right in the light blue area. Some departments inside your organisation may be at different levels than others.

The GDPR compliant solution matching the needs is recommended in the blue area. In the white area the GDPR compliance argumentation is to be found.

Customer's situation	Level 1 Basic	Level 2 Basic external provider	Level 3 Print, Copy and Scan	Level 4 High Availability
Customer Scenario and Needs	All printers are personal printers attached directly to the users' workstations or all printers are very close and visible to the users Copying and scanning are either impossible or under surveillance	All printers are personal printers attached directly to the users' workstations or all printers are very close and visible to the users Copying and scanning are either impossible or under surveillance Data travels outside premises to e.g. data center	Company printing, copying and scanning personal data Printing, copying and scanning are not critical processes (not business blocking if printing is down for a short period) Printers physically placed in printing separate rooms Copying, scanning and maybe faxing Printing from mobile devices Printing from host computers (mainframe, AS/400)	Company printing, copying and scanning personal data Printing, copying or scanning are critical processes: - Risk of insecure user workarounds (e.g. print, copy or scan not through the solution) Printers placed in printing rooms Copying and scanning possible Printing from mobile devices Printing from host computers (mainframe, AS/400)
Customer Profiles and Examples	Small companies like shops and agencies Certain internal departments in larger companies	Companies with a cloud strategy Small departments geographically separated from server	Most companies: - Transportation, Logistics, Service, Food, Production etc. Companies usually have mixed printer technologies from different vendors Complex infrastructure, multiple locations	Healthcare and Finance Sectors Certain governmental companies Need for close to 100% availability and performance
One Q built-in security measures ensuring GDPR	**Accountability:** Activity Reports and Audit Trail about users, documents and when printing: - GDPR Auditing - In case of a GDPR breach Data Protection by design: - Newest secure components - Refactored code (no back doors) - Data minimization: No redundant user credentials Storage limitation/Right to be forgotten	**Level 1 and:** Data Protection by design Certificate based end-to-end encryption	**Level 2 and:** Activity Reports and Audit Trail expanded with copy, scan and fax Data Protection by design: - Integrity and confidentiality: Secure release of print jobs (follow me) - Data minimization: Not collected print jobs deleted automatically Purpose limitation: Data access on a need to know basis: - Delegated administration with One Q admin roles	**Level 3 and:** Data Protection by design High availability, high performance redundant setup with load balancing and failover, avoiding insecure alternative user behavior (e.g. installing unauthorized print drivers, copying using mobile phone camera etc.)
Recommended One Q Solution for GDPR Compliance	Tracking Push print One Q Print Monitor on the workstations for handling personal printers	Tracking Push print One Q Print Monitor on the workstations for handling personal printers and encryption from workstation to printer SaaS on Azure solution for: - ISO 27001 certification - Geographical guarantees - Data Processor assurance	Secure software clients on MFP devices Secure release print on all printers Software on the workstation (One Q Print Monitor) for handling personal printers and encryption from workstation to printer Administrators organized with individual/ group rights Optional: - One-driver for all workstations - Secure cloud or mobility printing - Integration with secure print from host (IBM mainframe or AS/400) making this print equally secure	Clients on MFP devices 'Release all' solution on printers Print Monitor for handling personal printers and encryption from workstation to printer One Q Print Monitor for secure offline printing Administrators organized with individual/ group rights Failover Solution Load balancing on the servers Optional: - One-driver for all workstations - Secure cloud or mobility printing - Integration with secure print from host (IBM mainframe or AS/400) making this print equally secure
Additional measures to consider related to GDPR	Disposal policy for MFPs and printers with hard drive On-premise solution: Server must be security patched Customer is both Data Controller and Data Processor	Disposal policy for MFPs and printers with hard drive Customer is Data Controller Host/Cloud provider is Data Processor	Disposal policy for MFPs and printers with hard drive Customer is Data Controller Host/Cloud provider is Data Processor	Disposal policy for MFPs and printers with hard drive Customer is Data Controller Host/Cloud provider is Data Processor

Do you want to know more?

Ask for GDPR guide advice

gdpr@oneq.tech

+45 70 20 32 84