ThinPrint®

EU General Data Protection Regulation:

What to Consider for Network Printing

Contents

Caution: Data Protection Risks for Network Printing

The European General Data Protection Regulation (EU GDPR), introduced in May 2018, has harmonized the rules for processing personal data by private companies and public bodies across the EU. Especially in small and medium-sized enterprises however, there are still some uncertainties regarding the EU's legislation. What information is to be assigned to personal data? Which IT processes are affected? Where do you start with the implementation? For example, companies and public authorities in Germany are already very well positioned with the Federal Data Protection Act. Nevertheless, existing IT processes often need to be further optimized or security deficiencies remedied. In the course of this, printing processes in the company should also be scrutinized.

According to the GDPR, natural persons have a right to protection of their personal data (Article 1 (2), GDPR). The harmonization of regulations facilitates the processing of personal data across national boundaries, since national data protection regimes, which have until now contained differing regulations, will no longer constitute an obstacle (Article 1 (3) GDPR). But how to recognize whether certain data or information is considered personal data or not? Data falls into the category of personal data when a person can be directly or indirectly identified, for example by means of their name, their telephone number, account data, postal or IP address.

The right to protection of personal data is to be protected by Art. 5 GDPR
(Principles on the processing of personal data). This results in extensive documentation obligations for companies and they are obliged to report data leaks in a timely manner. Additionally, violation of the data protection directives is subject to very high fines.

Frequently, it is often overlooked that significant security risks concerning personal data also exist during the printing process:

›

- Unencrypted transmission of personal data over the network
- Unencrypted storage of personal data during the printing process on servers or printer hard drives
- Output of confidential documents to the wrong printers
- Documents containing personal data falling into the wrong hands at the printer

With ThinPrint, you can fully secure printing processes, ensure GDPR compliance and eliminate data protection weaknesses without the need to invest in costly new hardware. Take this opportunity to learn how to secure the entire printing process against data protection risks in this white paper. Here's how to make your IT organization GDPR-compliant.

Network Printing – Background Information

1. Programs

In each print environment, the print job is started in the respective application. It runs either directly on the corresponding workstation (image 1) or on a Remote Desktop Session Host, a Citrix Virtual Apps server, or a virtual desktop. (image 2)

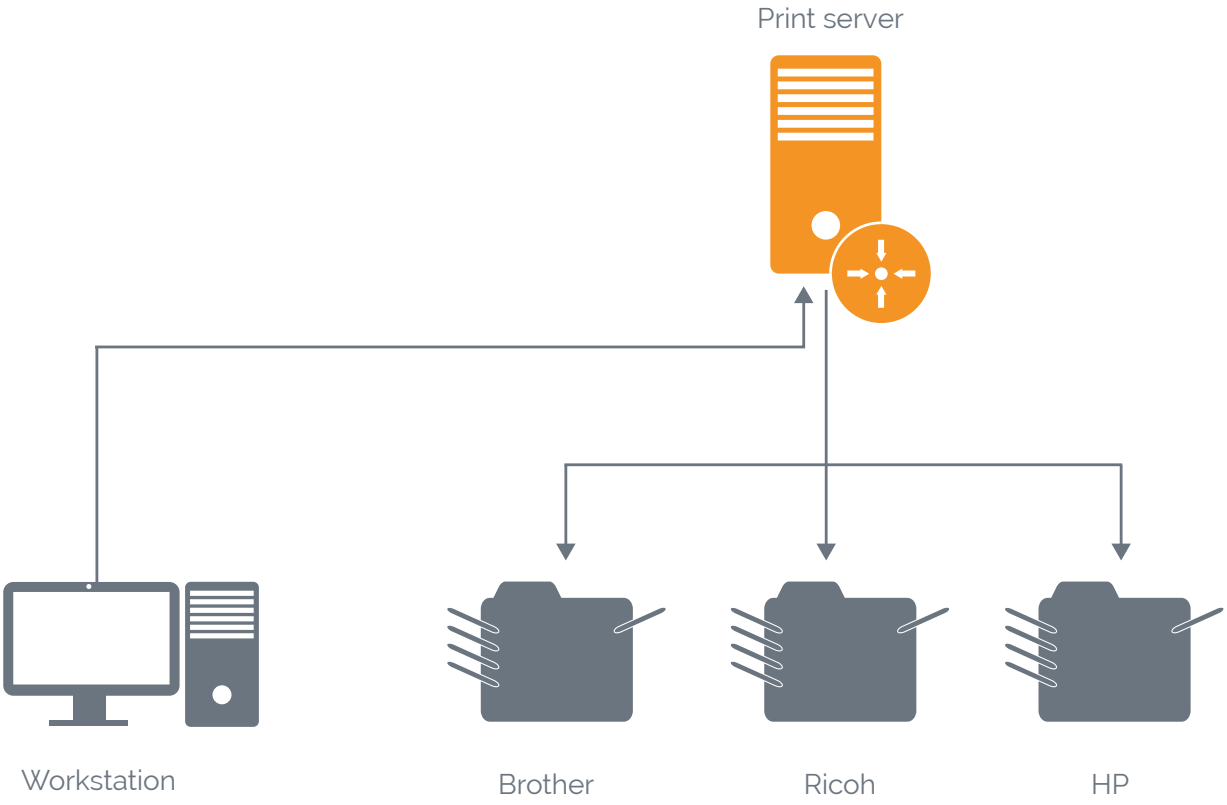

Image 1: Print data path from the program via the print server to the network printer

2. Print Servers

In medium to large print environments, print servers are used to centralize the printing processes. This not only simplifies administration, but also makes it possible to implement security technologies.

3. Network Printers

For administrative and cost reasons, many workplace printers have been replaced by network printers in recent decades. This often results in sensitive data being sent over the corporate network.

Network Printing Weak Points

IT administrators secure programs and data through access protection1, as well as through encrypted connections to servers and workstations. On the other hand, print data is often sent unsecured to print servers and from there to network printers. This results in the following weak points:

- The network cards of all devices over which the print stream travels: workstation, desktop, hub, router, server, and network printer
- The printers shared on the print server
- The hard drives of the network printers

Art. 4 + 9 GDPR:
Processing special categories of personal data

Article 30 GDPR:
Principles on processing activities

Print Data Encryption

There are several points where the printing process needs to be optimized in order to achieve comprehensive, secure print data encryption that is compliant with GDPR.

1. Program → Print Server

From SMB 3.0 onwards, print data can be encrypted by the program for printer sharing on the print server with Windows' native capabilities (image 2).2 This ensures that access to the shared printers on the print server is only possible via encrypted connections.

Article 5 GDPR:
Confidentiality and integrity

Article 32 I(a) GDPR:
Secure processing

1 for both application servers and workstations, but also for file servers and databases
2 Requirements: At least Windows Server 2012 or Windows 8

2. Print Server → Network Printers

Only third-party solutions can be used for connections from the print server to network printers. Solutions from individual printer manufacturers result in an increased administrative burden because they have to be installed and managed per printer manufacturer on the print server. A universal, manufacturer-independent solution that is also compatible with a wide variety of Active Directory structures is provided by ThinPrint (image 2).

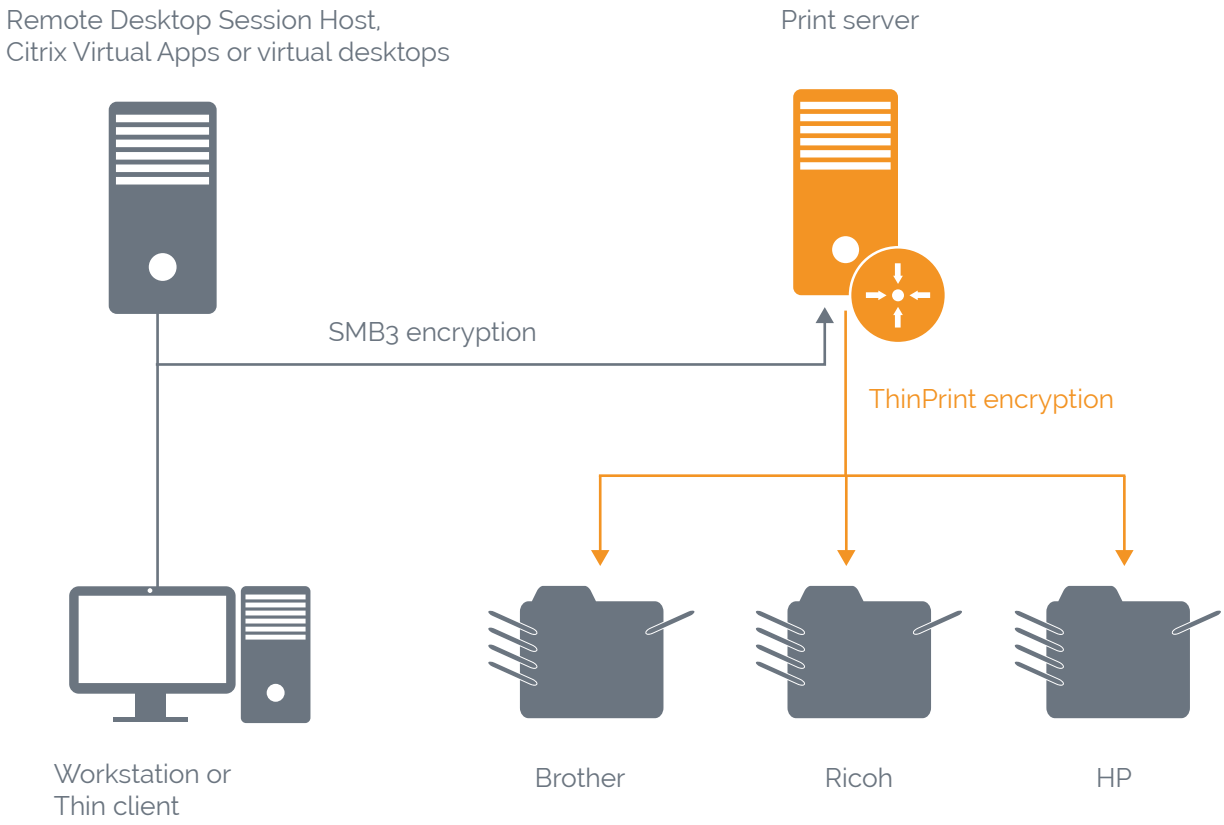

Image 2: Encryption of the print data from the program to the print server and from there to the network printers

For printer models that are not (yet) supported by ThinPrint, the **ThinPrint Hub** can be used, which forwards the print data to the network printer via USB. (image 3)

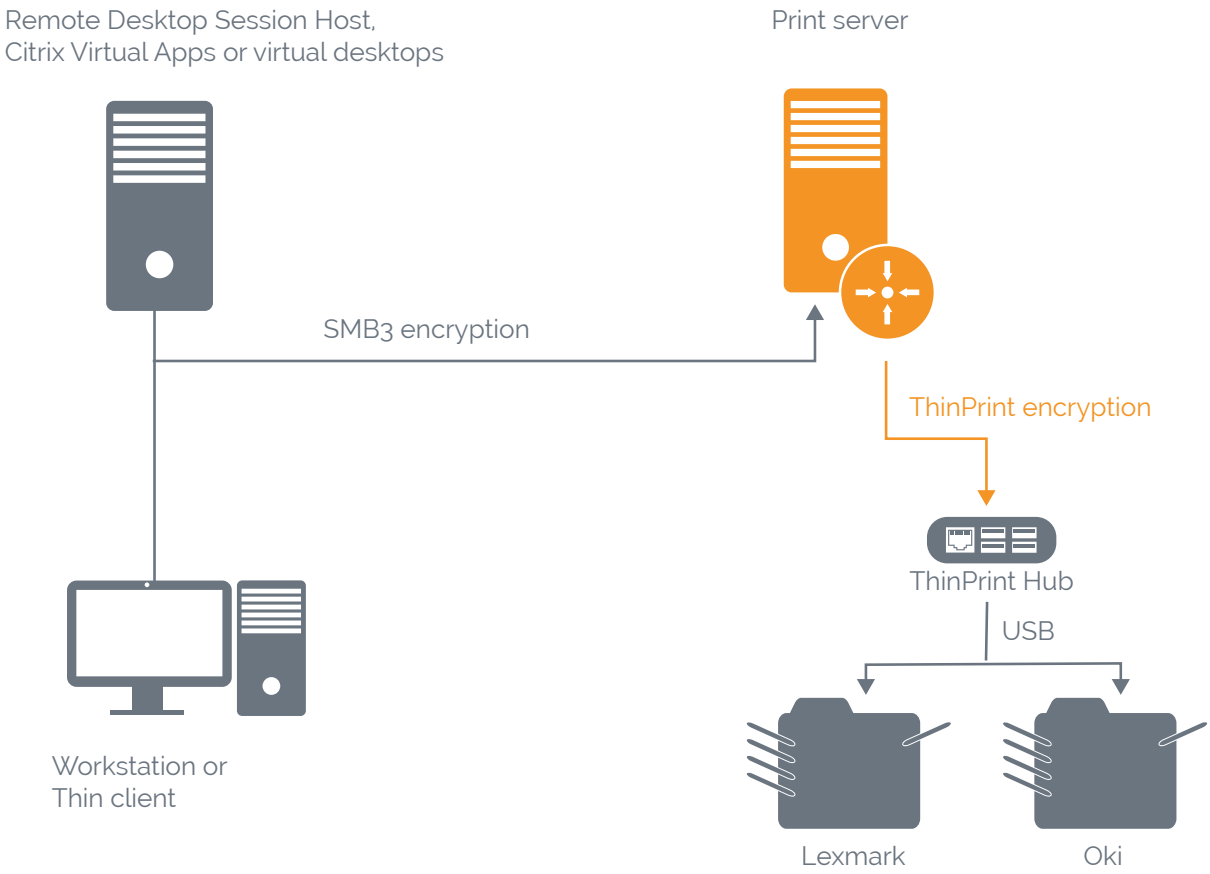

Image 3: Encrypting print data from the program to the print server and from there to the ThinPrint Hub

3. Network Printers

At the network printer itself, it must be ensured that unauthorized persons cannot log into the printer interface. To do so, certificates should be used which require a username and password. If the internal hard drive of the printer is used, then this must be encrypted (on the hardware side). Theft of finished printouts from the output tray can be prevented by user authentication directly at the printer. ThinPrint offers a variety of authentication options with Personal Printing including smartcard, smartphone as well as PIN authentication.

Article 32 GDPR:
Secure processing

The European Union’s General Data Protection Regulation: How to Ensure Compliance when Printing

It is essential that companies also pay attention to the complete printing process when reviewing data protection-relevant processes.

As shown in this white paper, a print job runs through different stations from the time it is triggered to the final printout. The individual stages are illustrated in this white paper. Existing security risks and weaknesses have already been highlighted.

It has been made clear that the connection from the print server to the network printer can only be protected by third party solutions. This results in a high administrative burden since the printer manufacturer solutions must be installed and managed individually on the print server. The network printer also presents a security risk. When the print job arrives at the network printer, it is not guaranteed that it will end up in the right hands.

ThinPrint is a professional, manufacturer-independent print solution, with which you can easily eliminate the weak points documented here. With ThinPrint, you can make your printing environment GDPR-compliant, without additional administration effort.

Appendix

Extracts from the EU's General Data Protection Regulation

Article 4 GDPR

For the purposes of this Regulation: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Article 5 GDPR

1. Personal data shall be:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
   (f) 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').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 9 GDPR

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply in the following cases: ...

Article 30 GDPR

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

   (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
   (b) the purposes of the processing;
   (c) a description of the categories of data subjects and of the categories of personal data;
   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
   (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
   (f) where possible, the envisaged time limits for erasure of the different categories of data;
   (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Article 32 GDPR

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 83 IV(a) GDPR

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b) the obligations of the certification body pursuant to Articles 42 and 43;
(c) the obligations of the monitoring body pursuant to Article 41(4).

Article 83 V(a) GDPR

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to EUR 20 000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

Abbreviations and Links

GDPR	European Data Protection Regulation
EU	European Union
GDPR	General Data Protection Regulation

For more information on ThinPrint encryption, including an overview of network printers with an integrated ThinPrint Client, please visit:

blog.thinprint.com/end-to-end-encryption-hp-printers

Infringement Against: ...	Administrative Fine:
Art. 5 GDPR	up to EUR 20 million or 4% of the world wide annual turnover pursuant to **Art. 83 V(a) GDPR**
Art. 9 GDPR	up to EUR 20 million or 4% of the world wide annual turnover pursuant to **Art. 83 V(a) GDPR**
Art. 30 GDPR	up to EUR 10 million or 2% of the world wide annual turnover pursuant to **Art. 83 IV(a) GDPR**
Art. 32 GDPR	up to EUR 10 million or 2% of the world wide annual turnover pursuant to **Art. 83 IV(a) GDPR**

Other white papers:
This and many other white papers on interesting IT topics can be downloaded free of charge from our website:
www.thinprint.com/whitepaper

Do you have questions?
The ThinPrint team will be happy to help you. We are available at the following telephone number:
+49-(0)30-39 49 31-0 or simply send us an email to **info@thinprint.com.**

Headquarters

ThinPrint GmbH
Alt-Moabit 91 b
10559 Berlin, Germany
Phone: +49 (0)30-39 49 31-0
Fax: +49 (0)30-39 49 31-99
email: info@thinprint.com
www.thinprint.com

ThinPrint by Cortado Pty Ltd. Australia
Level 10 I 20 Martin Place
Sydney, NSW 2000
Australia
Phone: +61 2 9639 6643

USA (Colorado)

ThinPrint, Inc.
3827 Lafayett St #130
Denver, CO 80205
Phone: +1-303-487-1302
email: info@thinprint.com
www.thinprint.com

ThinPrint Japan Japan
6F Shinmakicho Building
1-8-17 Yaesu
Chuo-ku Tokyo
Post Code 103-0028
Japan
email: info@thinprint.com
Phone: +81 3 5542 1551

ThinPrint®

Folgen Sie ThinPrint auf: facebook twitter youtube linkedin