Guide to GDPR-compliant printing

Printing, scanning, faxing, copying

Bitkom Guide

www.bitkom.org

bitkom

Publisher

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
(Federal Association for Information Technology, Telecommunications and New Media)
Albrechtstraße 10 | 10117 Berlin
P +49 (0)30 27576-0
bitkom@bitkom.org
www.bitkom.org

Contact person

Dr. Roman Bansen | IT-Infrastructure
P +49 (0)30 27576-270 | r.bansen@bitkom.org

Responsible Bitkom entity

AK Printing Solution Services

Authors

Dr. Roman Bansen | Bitkom e.V.
Robert Duisberg | Insentis GmbH
Bernd Hausmann | ThinPrint GmbH
Sabrina Heidgen | Ricoh Deutschland GmbH
Dennis Klussmann | Lexmark Deutschland GmbH
Christoph Losemann | Canon Deutschland GmbH
Carsten Meerpohl | Kyocera Document Solutions Deutschland GmbH
Jochen Plehnert | Konica Minolta Business Solutions Deutschland GmbH
Stefan Rautenbach | Ricoh Deutschland GmbH
Marc Recktenwald | HP Deutschland GmbH
Dr. Carsten Rückert | Wilhelm Dreusicke GmbH & Co. KG
Daniel Schiwek | HP Deutschland GmbH
Andre Schnibbe | SEAL Systems AG
Hans-Michael Voss | Lexmark Deutschland GmbH
Rebekka Weiß | Bitkom e.V.

English translation

Xerox GmbH

Cover image

© Ana Rivarola – unsplash.com

Content

List of figures

1 Introduction

1 Introduction

For some years, the EU General Data Protection Regulation (GDPR) has been the binding legal framework for the protection of personal details. The GDPR is able to impose severe sanctions; in the case of (serious) violations, eight-figure euro fines have already been applied on many occasions.

It is therefore absolutely essential for companies to ensure that every employee and department really does treat personal data in a GDPR-compliant manner. Printers and multifunction devices that are able to copy, fax and scan (hereinafter called »printers« and »printing systems«) are prime examples of systems at companies that often receive attention last of all.

Nonetheless, these devices also process personal data – and they do so in two ways. First, personal data (e.g. a username) is processed in a variety of ways, during the technical printing process, between sending something to print and getting a printout. This kind of data is known as transaction data. Second, the documents being printed also generally contain personal details. This kind of data is called user data.

This poses the question as to whether GDPR-compliant printing solutions can actually be purchased »off-the-peg«. Achieving GDPR compliance is, to a large extent, a process to be implemented on an individual case basis, with the characteristic features and specific details of each company necessarily occupying a central place. Usually, this calls for cooperation between specialists, technical experts, data protection specialists and legal experts in order to create an effective and sustainable concept for GDPR compliance.

It must also be borne in mind that evidence to verify GDPR compliance measures may need to be provided at any time (e.g. to government bodies or auditors).

This guide highlights the aforementioned aspects that need to be considered in relation to achieving GDPR compliance. During implementation, it can be helpful to draw upon external expertise.

The guide is also available in German. You can find both versions under the following link:
↗www.bitkom.org/Bitkom/Publikationen/DS-GVO-konformes-Drucken

2 GDPR

2 GPDR

2.1 GDPR – What is it, and why is it so important?

The General Data Protection Regulation (GDPR) entered into force in 2016. It entered effect across the entire EU in May 2018, and it has been possible to impose sanctions under the GDPR as of this date. It governs the processing of personal details of natural persons in the EU on a global basis for all companies and organisations.

The GDPR applies only to personal data. This includes all information that can be used to identify a person directly or indirectly. Important points of the GDPR include the obligation to provide documentation of measures adopted, as well as a reporting obligation in relation to violations and infringements.

2.2 What are the potential consequences of data protection failures?

In the press, you can occasionally read of GDPR violations and of the financial penalties imposed as a consequence. Therefore, this regulation should never be viewed as a toothless tiger. In the first year after it entered into force, data protection officers in the German federal states took action in relation to no fewer than 81 cases of GDPR violation. In a direct comparison with other EU countries, Germany was fairly reticent, at least to begin with, especially in terms of the fines it imposed. However, in November 2019, a fine was imposed that broke the one million euro barrier in Germany for the first time. Since then, fines have been rising rapidly. It must be remembered that companies who have been issued such fines can also request confidentiality in relation to their own actions. Consequently, only a tiny number of such cases ever enters the public domain.

2.3 Which principles apply to data processing?

The nature and scope of personal details that a company or an organisation may process in a GDPR-compliant manner depends on the purpose of that processing and the intended use. The following principles must be observed:

- **Legality, processing in good faith, transparency:** Personal details must be processed in a legally compliant and verifiable manner. Information provided to people whose details are being processed must be communicated in language that is easy to understand and that is readily accessible.

- **Appropriate use:** To process personal details, certain purposes need to be defined and the people whose details are being recorded or processed must be informed of those purposes. A company or organisation is not permitted to record personal details for undefined purposes, or to use that data for other purposes that are not compatible with the original purpose for which they were recorded.

- **Minimisation of data:** A company or organisation is only permitted to record and process personal details that are required to achieve the purpose.

- **Accuracy:** It must be ensured that personal details are factually correct and fully up to date in respect of the purpose for which they are being processed. If this is not the case, the details must be corrected.

- **Storage period:** It must be ensured that personal details are not stored for longer than is required for the purpose for which they were recorded, and that they are not stored for longer than the (statutory) storage obligations stipulate.

- **Integrity and confidentiality:** Appropriate technical and organisational measures must be taken to ensure the security of personal details, including their protection against unauthorised or unlawful processing and accidental destruction, damage or loss.

- **Accountability:** Companies and organisations are accountable to supervisory authorities in respect of GDPR. This means that, in cases of doubt, they need to be able to demonstrate that they are observing and applying the aforementioned principles, for example by providing evidence of appropriate procedures and processes.

- **Duty of disclosure:** Companies and organisations must provide individual information about the nature and scope of the processing of personal details to any person who may enquire about this. This information must be provided free of charge and without delay, within no more than one month of the enquiry. Information can be communicated in writing, electronically or – at the request of the data subject – verbally.

- **Right to deletion:** People have the right to request the deletion of personal details relating to them. In the absence of other higher-ranking regulations (e.g. statutory storage periods), deletion must take place without delay.

3 »GDPR-compliant printing«?

3 »GDPR-compliant printing«?

As the interface between the digital and the analogue world, printers and/or multifunction devices are accorded a special significance with regard to the GDPR. On the one hand, documents can include personal details and therefore data that is eligible for protection under the GDPR. In such cases, the processes involved must be designed to uphold the principles of the GDPR. On the other hand, a large volume of transaction data is generated during processing that can also contain personal details. In this context, it therefore follows that personal details need to be protected against unauthorised access by what are referred to as Technical & Organisational Measures (TOMs). This must always be borne in mind when disposing of old devices.

Similarly, attention must also always be paid to context and proportionality. It would, for example, be reasonable to assume that an access check at the printing system that involves biometric data (e.g. fingerprint) would constitute a pragmatic and secure authentication solution. However, biometric data in particular falls under the category of particularly sensitive personal data. The associated and immensely more comprehensive protection requirements for biometric data means that its use for conventional authentication purposes would appear to be proportional only in exceptional cases.

For that reason, all processes upon which a printing system is based, starting from its purchase to its operation and through to its disassembly, need to be designed in a way that is GDPR-compliant and that is integrated in the operational data protection concept. Due to the complexity of this topic, the individual organisational requirements and the large number of potential solutions, it is advisable to call upon specialist expertise.

It should be noted that GDPR-compliant printing is not available as a finished product. Instead, it is the result of a data protection concept that is founded upon the needs of the organisation involved; one that is well documented and implemented, as well as monitored continuously.

Further links:

- Text of the GDPR legislation: ↗https://eur-lex.europa.eu/eli/reg/2016/679/oj
- FAQ from Bitkom on the GDPR: ↗https://www.bitkom.org/Bitkom/Publikationen/FAQ-zur-Datenschutzgrundverordnung.html
- Bitkom overview page in relation to GDPR: ↗https://bitkom.de/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html

4 GDPR-related data in a printing context

4 GDPR-related data in a printing context

4.1 Overview and diagram

Having explained the pertinent provisions and regulations of the GDPR in the preceding sections, we now turn to the question of where data requiring protection may arise with regard to printing, copying, scanning or faxing. To this end, we consider the usual process flows relating to input, processing and output.

All of these process flows generate a significant volume of personal data – known as »transaction data«. The text of the document itself may also contain personal details – known as »user data«.

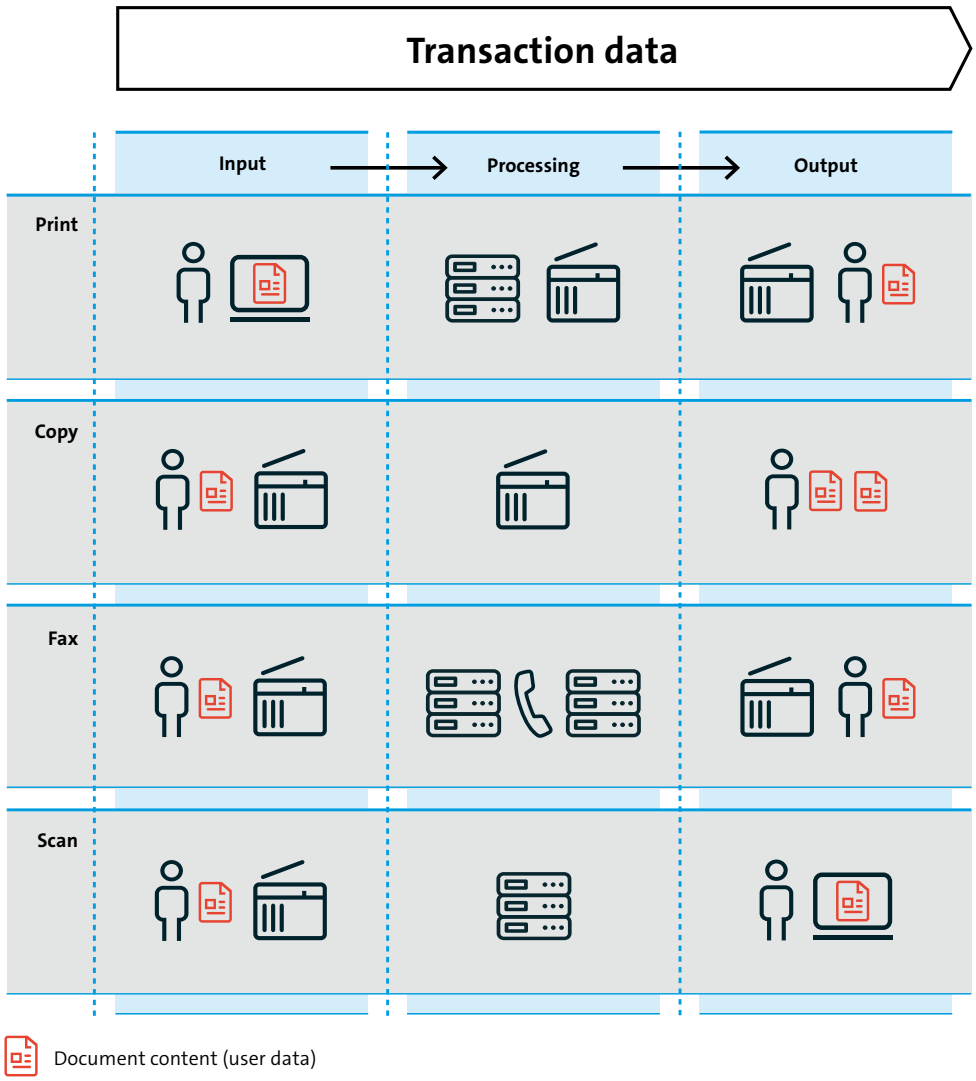

Figure 1: This diagram shows the fundamental differences between the individual functions

4.2 What specific GDPR-related data occurs?

As a reminder, the GDPR relates exclusively to personal details. This includes all information that can be used to identify a person directly or indirectly. It also includes data that is available in paper-based form. In contrast to anonymised data, pseudonymised personal details also fall under the scope of the GDPR because they can, in principle, be assigned to a defined person. This is because, with pseudonymisation, the related personal details can be reconstituted through the use of additional data.[1]

Personal transaction data is used during the entire input/processing/output process on printing systems, and includes actual names, login details, personnel numbers, IP addresses, MAC addresses etc.

Furthermore, additional personal details may be required in the overall process that are often sourced via the directory service in the network – this extends to login details for accessing third-party services (e.g. cloud-based services).

Another, not necessarily apparent, source of data is address books in the printing system that may store details such as internal or external phone numbers, personal e-mail addresses, and so on.

A high volume of personal details can also be found in the user data. Examples of items that may include GDPR-related data include invoices, personal documents or health data as well as circular letters.

In addition to the option of storing these documents to the systems concerned, the details they contain also constitute part of the printing or scanning data. A bulk or transaction print run (e.g. invoices, reminders) is often started and executed as part of a batch processing operation. Even though the individual documents being produced very much require protection, the user seldom has any scope to intervene directly during the mechanical printing and posting process (for batch processing operations). As a consequence, this entire process needs to have reliable quality control measures in place to detect potential violations of data protection provisions.

1 For details of the distinction between pseudonymisation and anonymisation, see page 31 onwards at the following link: ↗**https://www.bitkom.org/Bitkom/Publikationen/Machine-Learning-und-die-Transparenzanforderungen-der-DS-GVO.html**

4.3 The functions in detail

4.3.1 Print function

- In the first instance, this function is required to generate a print request for the document that is to be printed. This can be triggered by a user on a terminal device (PC, tablet etc.).
- In the processing operation, this request is then converted into a print job that the printer can understand and execute. Typically, this print job is then sent to join a predefined queue at a printer.
- During the output process, user authentication may be required at the printing system (e.g. by means of an access card). At that point, the selected print order is activated and the printout is issued to the output tray where it can be removed by the user.

	Input	Processing	Output	
Print	▪ Initiator, logged-in user ▪ Actual name ▪ E-mail address ▪ Personnel number **IT infrastructure & network security:** ▪ User ID, login account ▪ IP address, MAC address ▪ Subnet mask/location detection	▪ Database (e.g. circular letter, customer-specific user data) ▪ Device-specific log data ▪ Print data **IT infrastructure & network security:** ▪ Directory service ▪ System log data	▪ Authentication data (PIN, chip card, fingerprint,...) ▪ Printer ID	**Document content (user data)**
	Document content (user data)			

Figure 2: GDPR-related data involved in the printing function

For the following functions, the user authenticates the required operation at the printing system before being able to start a function. In detail, this involves:

4.3.2 Copy function

- Authentication, see above
- Insertion of the original and selection of the copy settings (number, one-sided/two-sided, required post-processing, etc.)
- Processing of the copy request
- Output of copies

	Input	Processing	Output	
Copy	▪ Authentication data (PIN, chip card, fingerprint,...) ▪ Initiator, logged-in user ▪ Actual name ▪ E-mail address ▪ Personnel number **IT infrastructure & network security:** ▪ User ID, login account ▪ IP address, MAC address ▪ Subnet mask/location detection	▪ Database (e.g. circular letter, customer-specific user data) ▪ Device-specific log data ▪ Print data **IT infrastructure & network security:** ▪ Directory service ▪ System log data	▪ Not applicable	**Document content (user data)**
	Document content (user data)			

Figure 3: GDPR-related data involved in the copy function

4.3.3 Fax function

- Authentication, see above
- Insertion of the original and entry of the fax destination
- Processing of the fax request
- Arrival of the fax at its destination; in most cases, with a direct printout option

	Input	Processing	Output	
Fax	▪ Authentication data (PIN, chip card, fingerprint,...) ▪ Initiator, logged-in user ▪ Actual name ▪ E-mail address ▪ Personnel number **IT infrastructure & network security:** ▪ User ID, login account ▪ IP address, MAC address ▪ Subnet mask/location detection	▪ Recipient number ▪ Transmission number ▪ Database (e.g. circular letter, customer-specific user data) ▪ Device-specific log data ▪ Print data **IT infrastructure & network security:** ▪ Directory service ▪ System log data	▪ Fax ID	**Document content (user data)**
	Document content (user data)			

Figure 4: GDPR-related data involved in the fax function

4.3.4 Scan function

- Authentication, see above
- Insertion of the original and entry of the scan destination (note: a security check of the scan destination may be helpful, or a restriction of the destinations that can be selected may be advisable)
- Processing through transmission of the scan and transfer to its destination

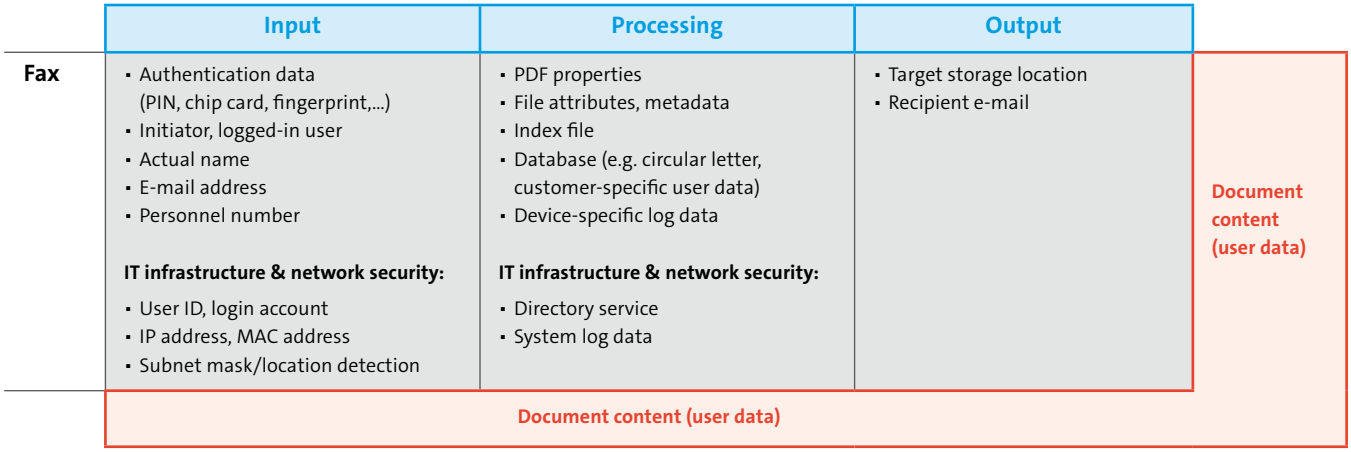

Figure 5: GDPR-related data involved in the scan function

The following graphic includes all of the aforementioned areas and data again in a clearly visible format:

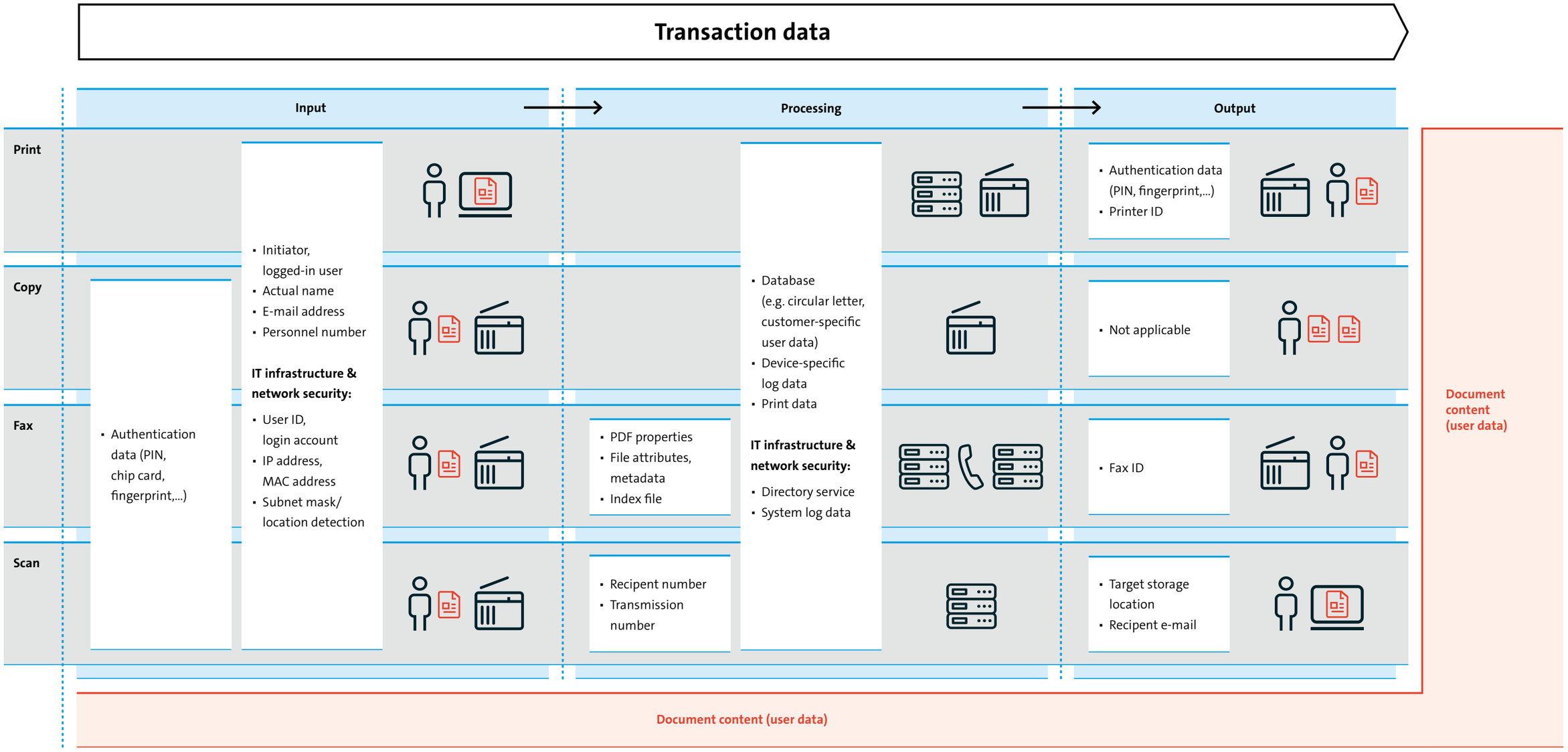

Figure 6: Functional diagram: Input – Processing – Output

5 How can GDPR compliance be achieved?

5 How can GDPR compliance be achieved?

5.1 Individual concept

Since there is no such thing as off-the-peg GDPR-compliant printing, there is a need to devise an individual, end-to-end concept for each company, one that also incorporates on-site measures (e.g. entrance and access checks to printer output). Above all, the technical and organisational measures need to satisfy the following criteria:

- The solution must be state of the art. This requirement is context dependent and therefore needs to be assessed on an individual basis. Fundamentally, this entails having a tried and tested practical model that exceeds the requirements of legislative stipulations or technical standards.

- The processing of personal details is permitted only if a corresponding GDPR-related permission status or a special legislative provision is satisfied. Each company is entitled to process the personal details required to perform its business purpose. Essential requirements in this regard are a precise description of the process and explicit measures to prevent any misuse of data whatsoever. It must be borne in mind that personal details may also exist or be provided in hard copy format during business processes, and this data must also naturally be protected in full.

- The time and effort required for these technical and organisational measures must be reasonably proportional to the level of protection required (the principle of proportionality).

- Key requirements include the complete implementation and continuous monitoring of the GDPR concept, together with a commensurate level of documentation. Sustainable implementation also includes, by way of example, regular employee training sessions and internal regulations that are binding upon all employees. This documentation is important for two reasons:

  1. To enable identified data protection violations to be logged on an ad hoc basis in order to ensure that the legally stipulated deadline of 72 hours for reporting a data breach can also be complied with.[2]

  2. To provide substantive and verifiable results of any spontaneous spot checks. Experience indicates that GDPR violations usually centre around one legal issue: »How intensively is the company endeavouring to protect personal details effectively against misuse?«

2 Art. 33 GDPR provides detailed information about whether or not the data breach has to be reported to the supervisory authorities as a statutory requirement

5.2 Examples of how you can protect data

5.2.1 Authentication – to protect against unauthorised access to personal details

Use an authentication process to protect your system against unauthorised access. GDPR-related data can be protected by preventing a document from being printed until an authorised user has logged in to that device, e.g. using an ID card or PIN code (»confidential printing«).

Authentication using biometric data is also possible in principle. However, that involves the permanent storage of biometric user data. Note that this data is classified as highly sensitive under the terms of the GDPR. A case-by-case check is required to establish whether authentication by means of biometric data is possible in relation to the defined purposes, the specific business processes and the protective measures that need to be implemented.

Under some circumstances, it may also be advisable to set up a user access check.

5.2.2 System administration – to protect against unauthorised users

Restrict the administrator rights for all systems involved in printing to as few users as possible. Alternatively, you can issue specific administrator rights to different roles. Functions should be available only to those users who need them for their work.

You should also perform regular software and firmware updates to close any security loopholes. If you have a large/remote fleet of printers, you can employ tools such as remote services or printer fleet management systems.

5.2.3 Restriction on the sending function – to protect against uncontrolled transmission to recipient addresses outside the organisation

The sending function should only ever be made accessible to users who genuinely need it. It is advisable to restrict the sending of documents to recipients who are listed in the address book or the LDAP server. Alternatively, sending can be restricted to the address of the logged-in user or to defined domains. This can reduce the potential risk of misuse of the sending functions (Scan to Mail, Scan to Fax) to a minimum.

5.2.4 Encryption of print data, documents and transport routes – to protect against access by unauthorised persons

When printing, scanning or faxing personal details, the document itself must be encrypted. Data should also be transmitted in encrypted form.

Independently of that, it must be ensured that the transmission routes are protected against unsolicited access. Technically adept users can find detailed information about this in the BSI Compendium of Basic IT Protection.[3]

5.2.5 Minimisation of volume and retention period of (interim) stored data – to protect against unauthorised access

Personal details in particular should be deleted immediately after processing by the system – from the printing system and also from the overall processing system as necessary. For this, it is advisable to carry out the rule-based deletion of storage media in accordance with international standards (e.g. BSI). As well as the rule-based deletion of data in temporary files during ongoing operation, the storage medium can be deleted securely at the end of its service life in various (manufacturer-specific) ways – if in doubt, by means of destruction.

5.3 Also pay attention to the following points or check their relevance

5.3.1 Clarification

Ensure that all people in contact with personal details observe the requirements of the GDPR in their daily work.

5.3.2 Data records

To be prepared for any requests for information from the data protection authorities, you should document the provenance, purpose and storage duration of all personal details. The processing directory acts as an important module for the traceability of data processing operations.[4]

5.3.3 Data protection statement

Always keep your data protection statement up to date by cross-checking it against current processing activities on a regular basis under consideration of its legal basis.[5]

3 ↗https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html

4 Detailed information about the directory can be found in the following Bitkom guide: ↗https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html

5 Instructions on how to produce a data protection statement can be found in the Bitkom guide to information-related obligations: ↗https://www.bitkom.org/Bitkom/Publikationen/Informationspflichten-nach-der-DS-GVO

5.3.4 Privacy laws

Check your business processes on a periodic basis to ensure that all individual rights relating to data protection are being upheld. If processing is being performed by external service providers, due observance of these rights must be covered in an order processing contract. Also ensure that the individual affected is informed of any such outsourcing of services.

5.3.5 Requests for information

Every natural person has a right to request information. Ensure that your processes comply with the relevant directives and regulations, and ensure that all requests for information about data kept on record and its intended purpose are answered within the statutory deadlines.

5.3.6 Consent

Check your procedure for obtaining, administering and handling personal data. Renew any existing consents that are no longer compliant.

5.3.7 Data protection violations

Ensure that you monitor your business processes to detect any data protection violations at an early stage and, if necessary, report them to the supervisory authorities. The obligation to report takes immediate effect and a report must be submitted within 72 hours of the violation being detected where possible.

5.3.8 Data protection officer

Check whether your company is legally obliged to appoint a data protection officer. Ensure that your officer is able to perform the defined duties properly. An external data protection officer can also be appointed.

6 Summary

6 Summary

The establishment of GDPR-compliant printing is a process that differs for each individual company and cannot be obtained »off the peg«.

Professional analysis of the business purpose is of paramount importance. From this, it can be established which personal details can actually be processed at all. The transaction details that occur during technical processes must also be taken into account. Based on this information, a concept with appropriate technical IT and organisational measures can be developed which ensures that the data technology is in place to process data in a GDPR-compliant manner.

This document provides just a few pointers relating to the most appropriate kind of information technology. Anyone wishing to learn more about the safe operation of printing systems would be advised to consult the **↗Bitkom guide »Security of printing systems«**[6].

However, it is important to remember that the GDPR construct is founded upon the principle of proportionality. There is therefore no need to »take a hammer to crack a nut«.

One fundamental point to bear in mind is that GDPR compliance is a dynamic process that can change often as time goes by, for example when opening up new areas of business.

6 **↗https://www.bitkom.org/Bitkom/Publikationen/Sicherheit-von-Drucksystemen**

7 Appendix – Fundamental definitions of terms

7 Appendix – Fundamental definitions of terms

7.1 Personal data – what is it precisely?

Under the terms of Article 4 (1) of the GDPR, personal data includes all information that relates to an identified or to an identifiable living person. Various items of sub-information that can, when taken together, identify a given person also constitute personal details. Personal data that has been encrypted or pseudonymised but that could be used again to identify a person continues to constitute personal data and falls under the range of application of the GDPR. Personal data that has been anonymised in such a way that the affected person cannot be identified, or can no longer be identified, no longer constitutes personal data. To ensure that this data really is anonymised, the anonymisation process must not be reversible.

The GDPR protects personal data irrespective of the technology used for processing that data – it is technology neutral and applies to both automated and manual processing, providing that the data is arranged in accordance with predefined criteria (e.g. alphabetic sequence). The way in which data is stored is also not relevant – it may be stored on an IT system, by means of video surveillance or on paper. In all of these cases, personal data is covered by the data protection clauses of the GDPR.

Examples of personal details**:**

- Surname and first name
- A private address
- An e-mail address such as firstname.surname@company.com
- A personal ID number
- Location data (e.g. the location function on mobile phones)
- An IP address
- A cookie identifier
- Pseudonymised data (enabling a personal reference to be reconstructed)

Examples of non-personal details:

- Company register number
- An e-mail address such as info@company.com
- Anonymised data (not enabling a personal reference to be reconstructed)

Examples of highly sensitive personal details:

- Biometric data
- Political convictions
- Sexual orientation
- Religious affiliation
- Health data

7.2 Processing of data – what precisely does that mean?

Under the terms of Article 4 (2) of the GDPR, “processing” covers a wide range of different processes relating to personal details, with or without the help of automated procedures. It covers the capture, recording, organisation, filing, storage, adaptation or amendment, interrogation, retrieval, use, disclosure through dissemination, distribution or any form of making it available to others, comparison or linking, restriction, deletion or the destruction of personal details.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

Federal Association for Information Technology, Telecommunications and New Media e.V.

Albrechtstraße 10
10117 Berlin
P +49 (0)30 27576-0
F +49 (0)30 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom