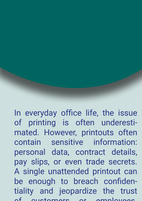
Wumbel™

Secure printing - an underestimated data protection risk



DR. BITTNER GROUP

In everyday office life, the issue of printing is often underestimated. However, printouts often contain sensitive information: personal data, contract details, pay slips, or even trade secrets. A single unattended printout can be enough to breach confidentiality and jeopardize the trust of customers or employees.

It is therefore important to handle print jobs consciously and securely.

Companies face the challenge of enabling efficient work while reliably protecting sensitive information.

However, this risk can be significantly reduced with clear rules, technical measures, and sensitized employees.

Discover why secure printing is an important part of data protection, what risks lurk in everyday office life, and how you can avoid data breaches with simple measures.

Why is printing a data compliance topic?

Printing means way more than just putting paper out. Every printout leaves the protected digital space and becomes a physical data carrier: readable by anyone and potentially accessible to unauthorized people. Typical risks in everyday office life include:

- **Printouts left unattended at the printer**
- **Misprints or test prints not disposed of properly (e.g., in normal paper waste instead of a document shredder)**
- **Documents are printed at the wrong printer or location**
- **Several people use the same printer without access restrictions**

Situations become particularly critical when personal data is involved. A document that is misplaced or viewed can quickly constitute a data protection violation. This can quickly have legal and financial consequences.

secure printing also means being responsible

The good news is that many risks can be avoided with simple rules of conduct and clear processes. Secure printing does not start with technology, but with employee awareness.

One of the most important rules:
Only start print jobs when you can go directly to the printer.

This prevents printouts from being left unattended or viewed by other people. This should become a fixed habit, especially for sensitive documents.

1 Classified documents need more care

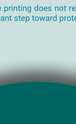
Not every document should be printed:
- **Is a printout really necessary?**
- **Does the document contain personal or confidential data?**
- **Is there a secure digital alternative?**

Fewer printouts automatically mean:
fewer risks, because paper
also has to be stored.

2 Use "secure printing" funcitonalities

Modern printing systems offer technical protection mechanisms:
- **Follow-Me-Print / Pull-Printing: Printing only takes place after logging in to the device (e.g., via PIN or chip).**
- **Access restrictions: Only authorized persons can trigger certain print jobs.**

Such functions ensure that documents are not left lying openly on the printer



3 Where your printer should be located

Care should also be taken when considering the right location:
- **Do not place printers in publicly accessible areas (e.g., reception, hallway, waiting area)**
- **If possible, place them in locked rooms or rooms that are only accessible to employees**
- **Sensitive departments (e.g., HR, accounting, management) should use separate printers**

4 Don't forget right disposal

What happens "after printing" is also crucial:
- **Confidential printouts do not belong in normal paper waste.**
- **Use document shredders or data protection bins.**
- **Even misprints are confidential documents.**

5 Raise employee awareness

Secure printing only works if everyone is on board:
- **Clear guidelines: What can be printed and what can't?**
- **Raising awareness that paper data is just as worthy of protection as digital information**

New employees in particular should be made aware of this issue at an early stage.

Wumbels dev tips!

Today's printers pose a real IT security risk. An important first step is to change the default passwords so that no one can gain unauthorized access to the internal memory and print jobs. Like other IoT devices, printers should also run on a separate network. This directly limits the potential damage in the event of an attack and protects sensitive data.

Conclusion: Data protection does not stop at your screen!

Every printout carries responsibility. With simple rules, technical solutions, and trained employees, the risk can be significantly reduced.

Secure printing does not require a great deal of extra effort, but is an important step toward protecting data, trust, and your company.

Dr. Bittner Consulting GmbH & Co. KG
Podbielskistraße 386
30659 Hannover
Servicenumber: 0800 88446688
Email: office@drbg.de

DR. BITTNER GROUP