PROTECT DATA!

§ About GDPR and ISO / IEC 21964

Guideline for paper documents containing confidential and personalised data.

IDEAL

Be careful with paper

When discussing data protection, people typically refer to electronically processed data. What is often forgotten: the provisions of GDPR also apply to personalised data in paper form. Do you know how you can protect your documents?

CONTENT

Play it safe!
Valuable practical tips regarding the destruction of confidential and personalised data on paper.

GDPR – General Data Protection Regulation.
Regulates the handling and processing of personalised data since May 2018.

NEW ISO/IEC 21964 and DIN 66399.
Supports data protection in business processes.

Information leakage in the waste paper bin: What type of firewall does your waste paper bin have?

70% of all important data is still written on paper. And these papers are often simply thrown into the waste paper bin. Data protection? No idea!

The following documents must be shredded when they are no longer needed:

- Quotations and contractual documentation
- Bank statements and records
- Invoices and receipts
- Personalised advertising documents
- Tax and accounting documents
- Signed documents
- Notes, print-outs, poor copies

THE SOLUTION

Integrate document shredders into your data protection concept.

In accordance with GDPR, you must demonstrate that you work compliantly and adhere to the data protection requirements. Protecting the required security level through the use of document shredders will protect you from paying significant fines, will protect your good reputation, and will ensure the trust of your customers.

What happens with your existing data?

Even your existing documents must correspond to the requirements of GDPR. Stocking up on data collection is prohibited.

PRACTICAL TIP

Update your documents regularly.

Data that may no longer be retained as per GDPR – keyword data minimisation – can be safely and reliably destroyed using a professional document shredder. Also keep in mind documents whose retention period has expired.

Information leakage: External service providers. What happens if data protection is left behind?

Do you have to regularly process large amounts of paper documents? It sounds enticing to have someone else handle both the work and the responsibility. However, this does not bring 100% security.

The risks:

- You do not see the result.
- Your documents are often temporarily stored before they are shredded.
- Service companies cannot release you from liability in cases of misuse.

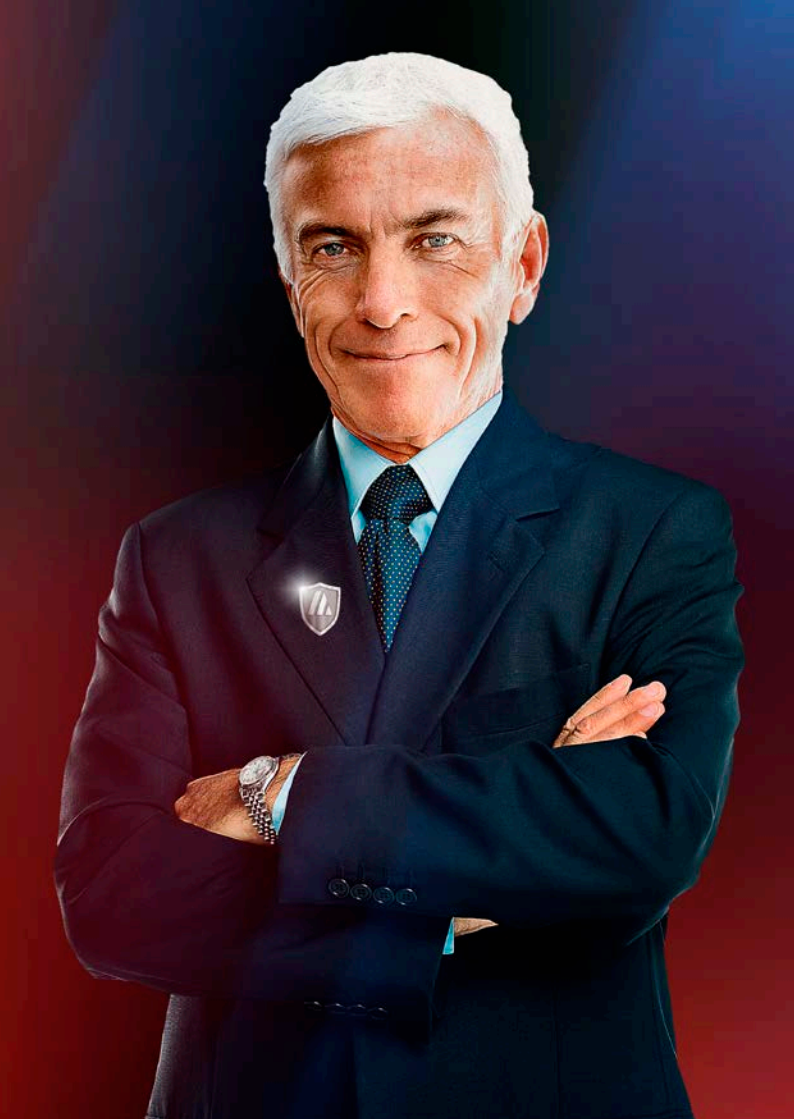
THE SOLUTION

Better do the shredding in-house.

No large collecting points, no long transportation routes, no hard-to-monitor intermediate stops: By shredding your confidential documents inhouse, these risks are eliminated. High-quality and high-capacity shredders work for many years – the investment pays off quickly. For violations against the GDPR, penalties of up to € 20 million or up to 4% of the company's global annual revenue are due.

SECURITY FOR ALL

So that my clients' confidential information remains confidential, I believe an office shredder made by IDEAL belongs to the basic equipment of every law firm. That's how you protect data.



Information leakage: the copying machine.

One copy: unaffordable?

Data protection begins with your daily tasks. Do your employees know what kind of data protection-relevant repercussions even slight negligence can have?

A typical office situation:

We allow our thoughts to drift – the confidential documents are inadvertently left in the copier and we only take the copies with us. Everyone who uses the copier has easy and unhindered access to our documents.

THE SOLUTION

Educate your employees.

Whether it's the papers left behind in the copier, or documents forgotten in the conference room: if personalised data lands in the wrong hands, then minor mistakes can result in major damage. If sensitive data is easily accessible for unauthorised third parties, you will be in violation of the data protection laws. A few simple copies can turn out to be really expensive.

Do I really need these copies?

A copy to read is quickly printed – and you might even make several copies of the latest draft contracts … Paper documents are difficult to monitor once these have been put into circulation.

PRACTICAL TIP

Avoid making unnecessary printouts or copies.
Only print out documents if this is absolutely necessary and pay attention to whom the documents are forwarded.

Information leakage: Your desk and inboxes.

End of work for data espionage.

On a daily basis, there are a lot of documents that pass across a desk – even documents that contain sensitive and confidential data. What happens with that data at the end of the day?

Every employee who does not leave a clean desk behind, will most likely grant access to unauthorised parties to gain access to confidential documents.

THE SOLUTION

Introduce a “clean desk policy”.

The instalment of a “clean desk policy” is an established system for all paper-based documents. Make your employees commit to sensibly file all documentation, to lock away all confidential documents, and to destroy all documents that are no longer needed. Using a deskside document shredder, you’ll be able to do this in one easy step.

SECURITY FOR ME

Aside from significant fines and targeted prosecution, a conflict or image loss can have astronomical consequences. With IDEAL shredders, I protect data – and I protect myself.

Data leakage: Your waste paper and rubbish bin.

Why could your waste paper be a treasure trove of information?

So-called „bin raiding“ refers to the practice of systematically searching waste paper and rubbish bins for exploitable documents and confidential data, with different intentions:

- Corporate espionage
- Identity theft
- Attempts at extortion
- Commercial fraud

THE SOLUTION

Introduce your individual data protection concept.

Ensure that you are aware of the processes in your company that involve confidential data, where this data goes and how it is destroyed. Alongside the decentralised use of shredders at particularly vulnerable workplaces, you may also find that it is necessary to position centrally placed devices. The only way to guarantee absolute security is by implementing a complete data protection policy that is adapted to your individual needs.

All this effort for a few pieces of paper?

The vision of a “paperless office” has not yet become reality. Although digitalisation simplifies many processes, it is generating more paper than ever before.

PRACTICAL TIP

Choose the correct shredder.

Always choose the devices “one size bigger” than required by the normal document quantity. This way you can comfortably and securely work when load pitches occur.

New ISO/IEC 21964

DIN 66399, which has been applicable in Germany since 2012, regulates data protection in business processes. The destruction of data has now also been globally standardised in the new ISO/IEC 21964.

You can easily determine the level of security you require in accordance with DIN or ISO by first identifying a protection class and then the appropriate security level.

Classification level 1

Normal sensitivity for internal data.
Security levels P-1, P-2, P-3

Classification level 2

High sensitivity for confidential data.
Security levels P-3, P-4, P-5

Classification level 3

Very high sensitivity for particularly confidential and secret data.
Security levels P-4, P-5, P-6, P-7

* Not applicable for personalised data

Internal data
Internal communication, such as instructions, forms or expired notices.

Sensitive and confidential data
Offers, purchase orders, order confirmations or delivery notes with address data.

Particularly sensitive and confidential data
Working documents, customer/client data, invoices, private tax and financial documents.

Data that must be kept secret
Balance sheets and P+L, strategy papers, design and engineering documents, personal data.

Secret high-security data
Patents, research and development documents, essential information that is important for your existence.

Top secret
Highly classified data for the military, embassies, intelligence services.

Material classifications

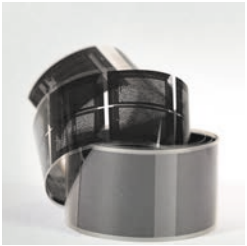
Next, select the data storage media that are relevant to you.

Alongside paper as a data storage medium, there are a number of other common data storage media that also feature in DIN 66399 and ISO/IEC 21964. See below for a short overview:

Information in original size

e.g. paper, films, printing plates.

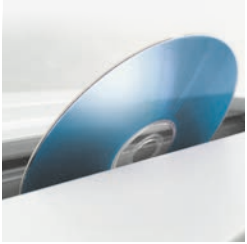
Security levels P-1 to P-7



Reduced information presentation

e.g. micro films, foil.

Security levels F-1 to F-7



Optical data carriers

e.g. CDs/DVDs.

Security levels O-1 to O-7

Magnetic data carriers

e.g. ID-cards, diskettes.

Security levels T-1 to T-7

Electronic data carriers

e.g. flash drives, chip cards.

Security levels E-1 to E-7

Hard drives with magnetic data carriers

Security levels H-1 to H-7

Information leakage: Hard drives.

Destroy old data carriers, not your good reputation.

Discarded hard drives are an open book for tech savvy “finders” – even if they have been overwritten. Once they have been disposed of, you can no longer verify where your old data carriers actually end up. And what happens to them.

Remember:

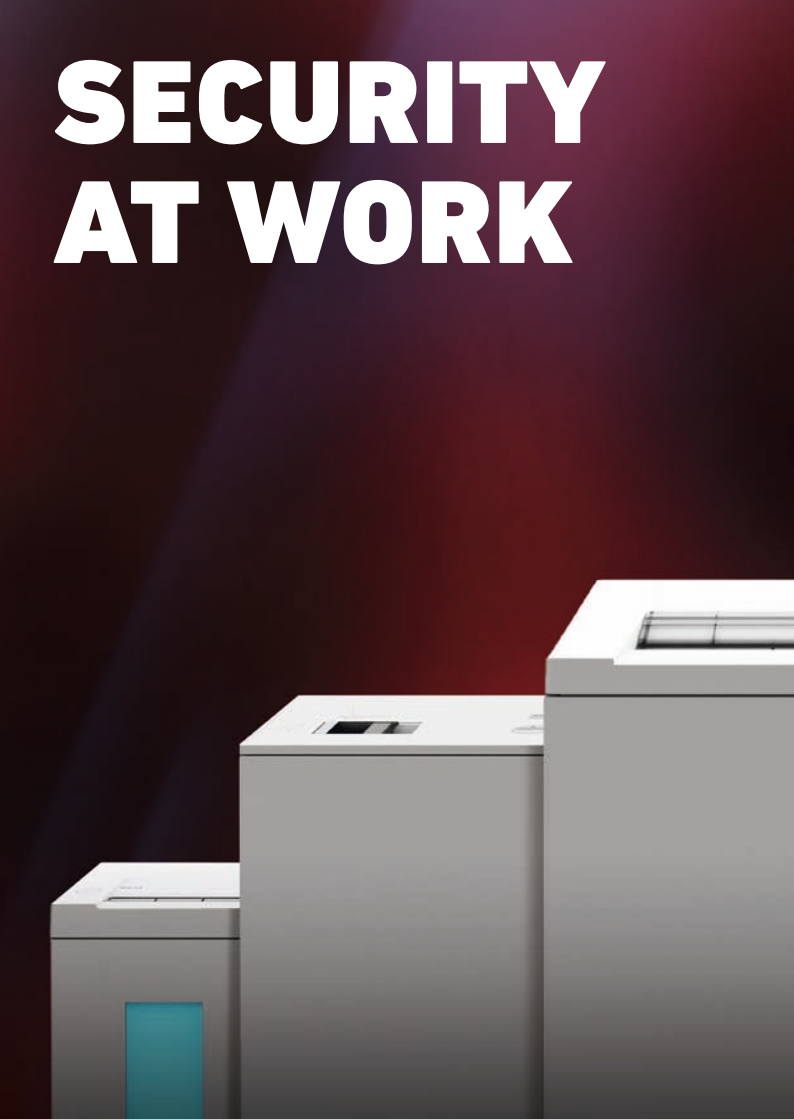
Hard drives are not only located in PCs and laptops, but also in printers, copiers and servers.

THE SOLUTION

Make your old data carriers unusable.

Regardless if you have to replace an old or defective hard drive, or if you have to return leased equipment: with a hard drive punch, you will destroy your discarded electronic data safely, comfortably and reliably.

SECURITY AT WORK



IDEAL document shredders reliably protect data. They are constructed to withstand the rigours of day-to-day office life. Companies, governments and organisations from around the world trust in that.

SECURITY SINCE 1951

Deskside document shredders

You should personally handle all of your personal data. Our deskside document shredders are ideal for individual workplaces or small work groups.
Data protection where confidential documents are created: right at your desk.

Office document shredders

Whenever high performance and a high shred bin volume are required, our office shredders are the first choice. They are suitable for centralised use. Ideal for large work groups, open-plan offices or an entire office floor.

High-capacity shredders

It does not matter how much paper needs to be shredded: You should always remain in control of your data and never surrender this responsibility to external disposal companies. IDEAL provides optimum solutions for in-house bulk shredding, too.

Special solutions

What happens to sensitive data stored on discarded hard drives? And what about smart cards, and optical data storage media? Our high-security devices are the perfect solution here. Ensuring your secrets stay secret for true peace of mind.

Always on the safe side

Quality does not come out of the blue.
It comes from IDEAL.
Made in Germany.

For additional information visit ideal.de

IDEAL

Subject to modifications and errors. FA 01.2019