PROTECTIT

Data Protection in everyday working live

Employee Training

Data protection training
Basics for employees

Welcome to the mandatory data protection training. In the next 60 minutes, you will learn the most important basics for legally compliant handling of personal data.

Goals of the training

Understanding Data Protectiton

Get to know and apply the basics

Strengthen responsibility

Raising awareness among employees

Practical tips

Recommendations for action in everyday life

Why Data Protection is important

Personal scale

Always ask yourself: “Would I be okay with it if it were my own data?”

Corporate risks

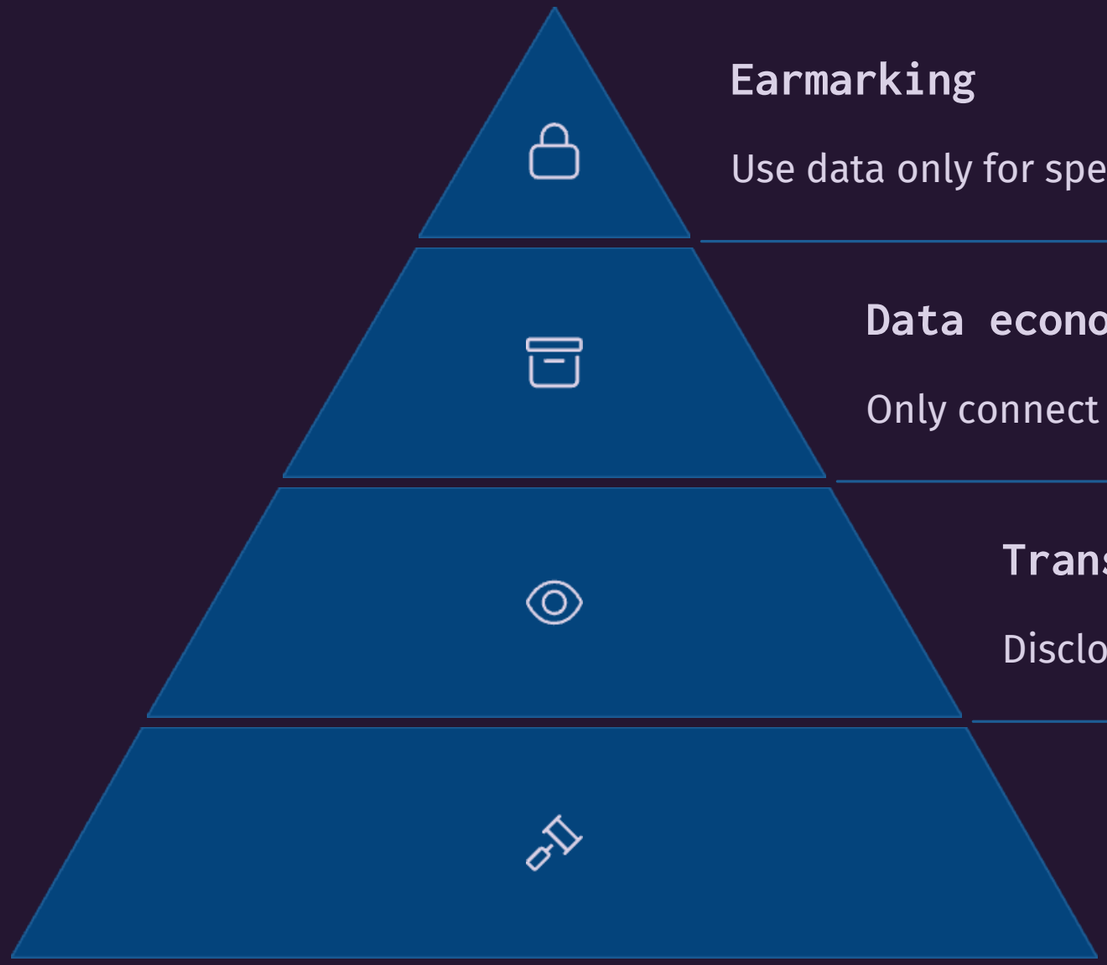
Data protection breaches lead to reputation damage and legal consequences.

Basis of trust

Customers trust us with their personal information. We must protect this trust

What is Data Protection?

Proteciton of personal data against misuse



Earmarking

Use data only for specified purposes

Data economy

Only connect necessary data

Transparency

Disclosure for data processing

Legality

Compliance with egal requirements (GDPR, BDSG)

Legal Framework

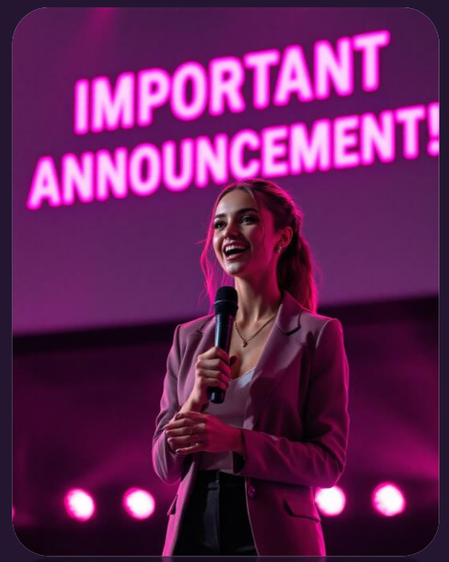
The General Data Protection Regulation (GDPR) has been the central European legal basis for data protection since May 25, 2018. It applies directly in all EU member states and creates uniform standards.

The Federal Data Protection Act (BDSG) supplements the GDPR at the national level in Germany. It specifies the framework of the GDPR and regulates specific requirements for certain sectors.

The Telecommunications and Telemedia Data Protection Act (TTDSG) has been in force since December 2021 and specifically regulates data protection in the area of electronic communications and online services.

There are special regulations for specific areas such as the Police Act for criminal prosecution and the Telecommunications Act (TKG) for providers of telecommunications services

Important terms in data protection



A comprehensive overview of the key concepts of data protection under the GDPR.

PROTECTIT

What is personal data?

Definition

Any information relating to an identified or identifiable natural person.

Examples

Generally:

name, address, date of birth

Bank details

Contact data:

E-Mail, telephone number, IP-Adresse,

Biometric data:

fingerprints, face recognition

Special categories

Health data, religious beliefs and other sensitive information.

PROTECTIT

Processing of personal data

Collect

Collect and record data

Store

Store and organize data

Delete

Delete and destroy data

Use

Reading and processing data

Controller and processor

Responsible

Determines the purposes and means of processing.

Contract

Regulates the duties and responsibilities of both parties.

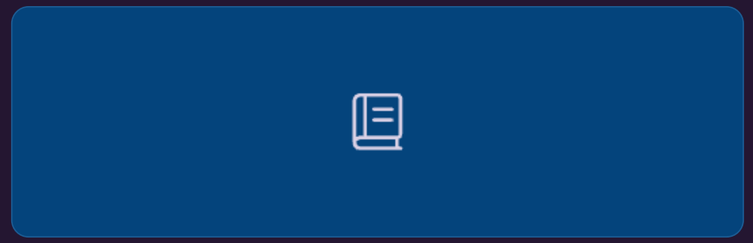
Processor

Processes data on behalf of the controller

The role of the DPO & the GDPR

Data Protection Officer

Monitors compliance with data protection



GDPR

Harmonizes data protection in Europe

Data protection in everyday life

Affects everyone and protects personal data

Rights and obligations

Rights of data subjects and corporate responsibility

Consent and rights of those affected

Consent

Must be voluntary, informed and unambiguous.

A clear affirmative action is required.

Rights of those affected

- Right to information
- Right to correction
- Right to deletion
- Right to data portability

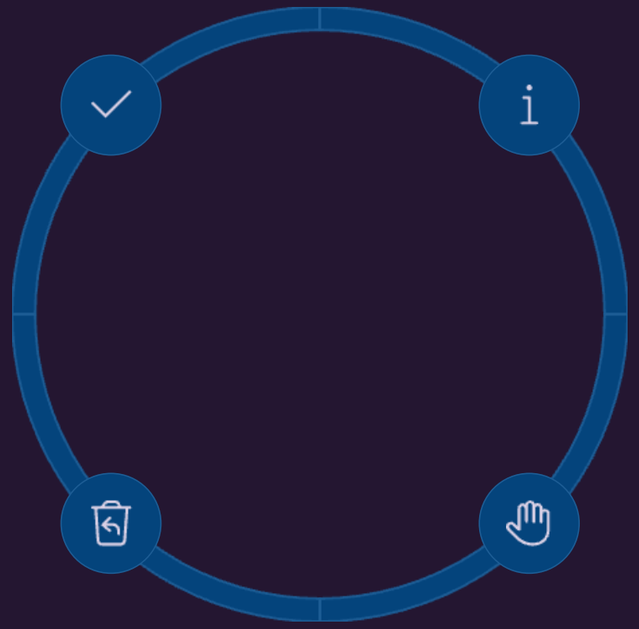
Consent: The Basis for lawful Data Processing

Voluntariness

Without coercion or disadvantage for refusal

Revocability

Possible at any time and without complications



Information

Full information about the purpose and scope

Clarity

Active action by the person concerned is required

Practical tips for obtaining consent

Clear forms

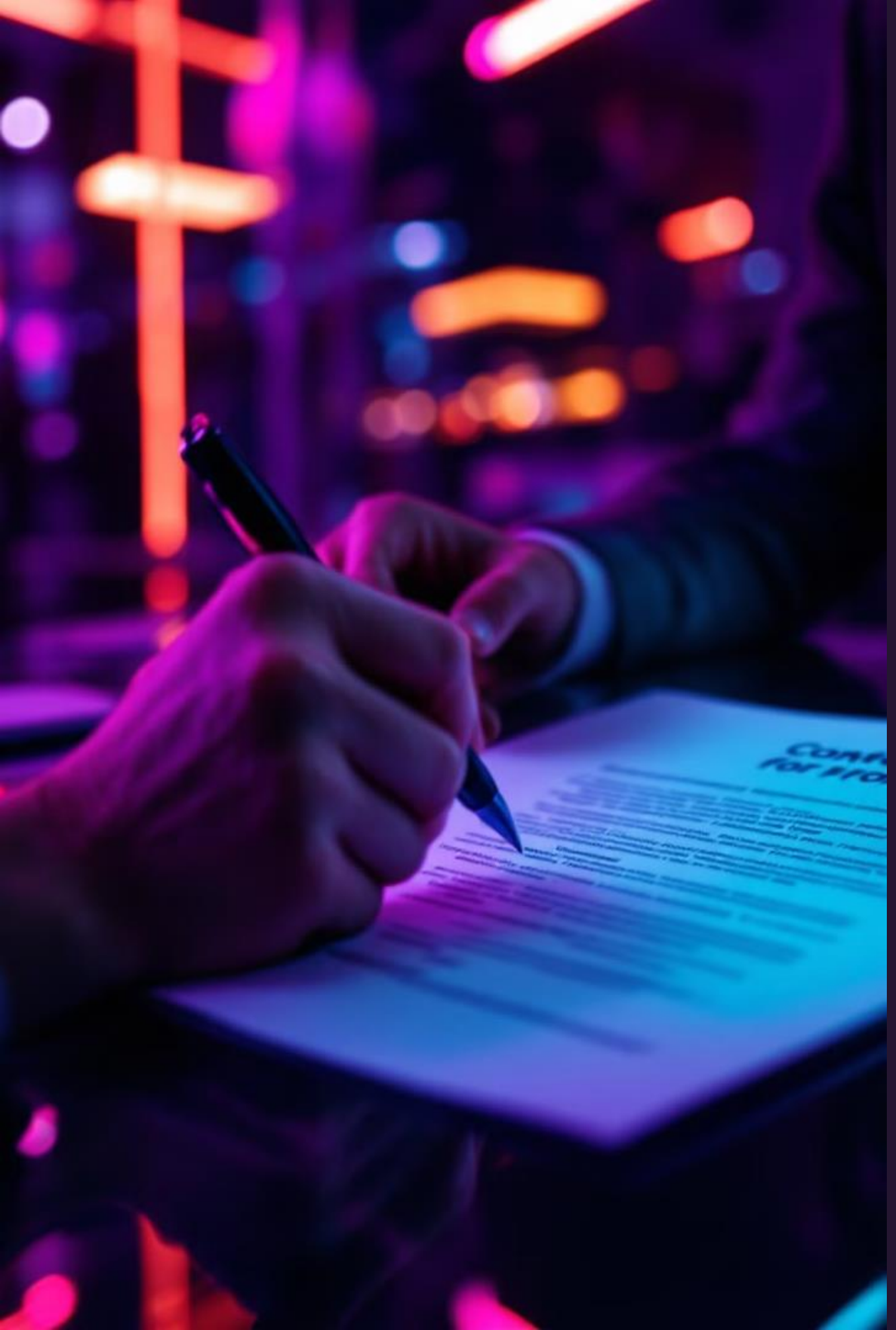
Clear design with simple language and clear options.

Specific purpose

Exact information about what the data is used for.

Careful documentation

Keep proof of consent given securely.



Fotos, videos & consent

Consent necessary

Always obtain written consent from identifiable persons

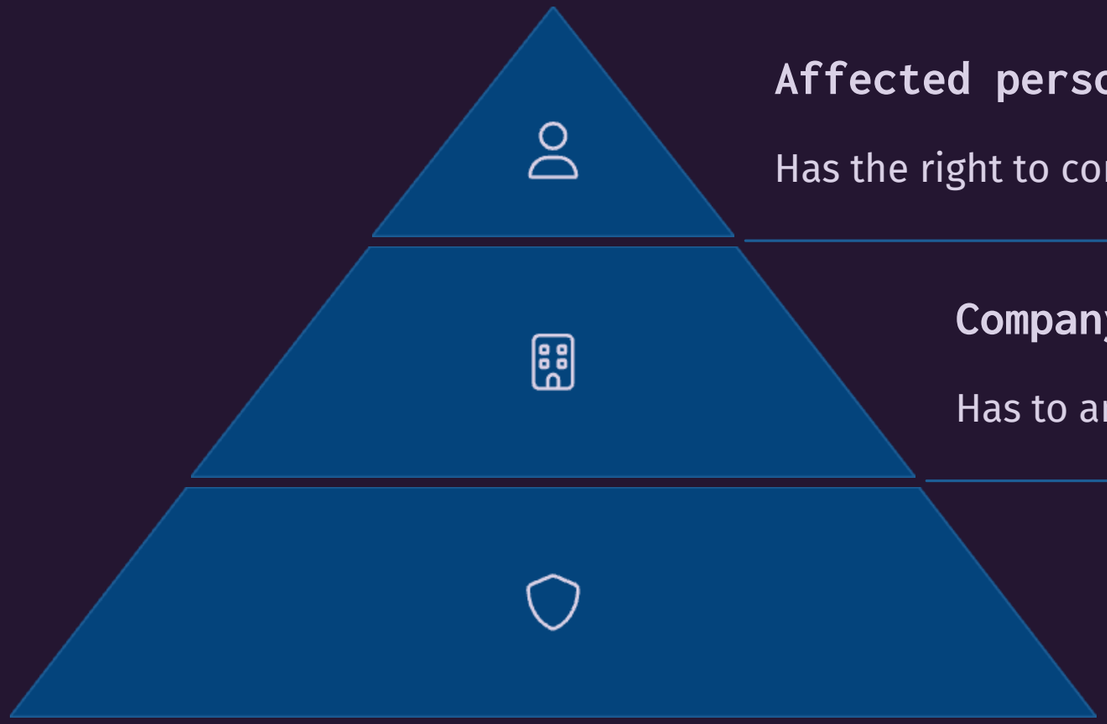
Documentation

Consent must be verifiable and retained.

Revocation

Individuals can withdraw their consent at any time.

Requests for information: A right of those affected



Affected person

Has the right to complete information about his data.

Company

Has to answer within a month

Legislature

Provides legal basis through the GDPR.

What to do if you request information?

Receipt of the request

Immediate forwarding to the DPC, DPO, and management. Documentation of receipt.

Proof of Identity

Ensure the requester is authorized. Beware of identity fraud.

Providing information

Ensure complete information within the statutory time limit.

E-Mail-Safety

Check sender

Report suspicious email addresses immediately

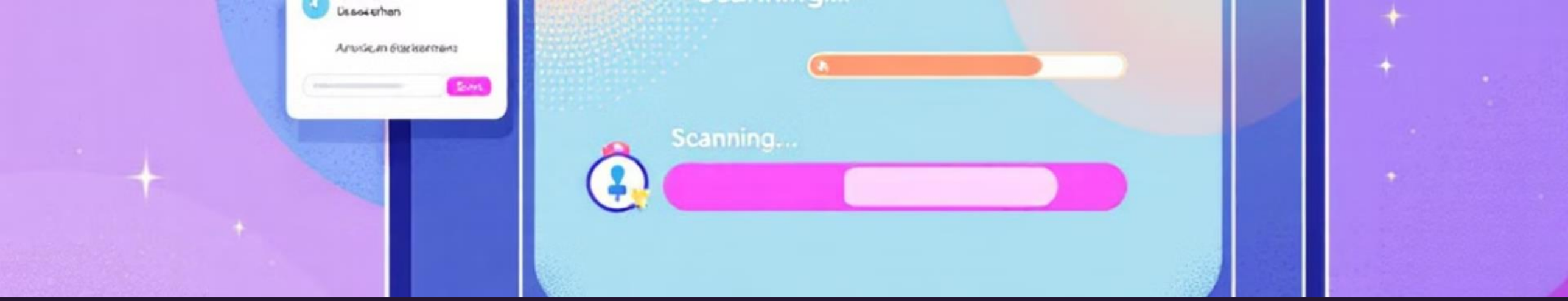
Control attachments

Do not open unexpected file attachments

Use BCC instead of CC

Protect email addresses in group emails

If you have any questions, contact the IT department. It's better to ask too many questions than too few.



Computer maintenance

Regularly updates

- Do not postpone OS updates
- Install software-updates in time
- Security gaps are closed quickly

Virus protection

- Keep Virus scanner always active
- Scan regularly
- Report suspicious files

Firewall

- Never deactivate the firewall
- Block unknown connections
- Regularly check settings

PROTECTIT

Screen lock and USB security

Activate Screen lock

Press Windows+L when leaving your workstation, even for short absences.

Do not use private USB-Sticks

Private storage media can introduce malware or cause data loss.

Use secure alternatives

Use company USB sticks or the company cloud for data transfers.

Password protection & IT security

Create strong passwords

At least 12 character, letters, numbers, special characters

Use a password manager

Secure management for all access data

Activate Two-Factor-Authentication

Additional security layer through second factor

Keep software up to date

Install updates promptly

PROTECTIT

Physical data security

Safe Storage

Files belong in lockable cabinets

Safe Disposal

Always shred confidential documents

Regular testing

Control of security measures

Clean Desk Policy

Keep your workspace tidy when you are away

Handle paper documents safely

Storage

Documents and personal files belong in lockable cabinet

Clean-Desk-Policy: Keep your workspace tidy

Protection from inside

Do not leave sensitive documents lying open

Turn over documents during conversations

Disposal

Use a document shredder for sensitive documents

No documents in the “normal” waste paper

Data protection during conversations and meetings

Maintain confidentiality

No sensitive conversations in public areas

Spatial demarcation

Close doors, screen not visible

Back up logs

Protect and archive documents quickly

Visitor management & behavior

Customer visits only with accompaniment

Visitors are never allowed to walk through the company unattended.

Discretion in public

Do not discuss customer data or internal information in public areas.

Be careful on social media

Do not mention company information or customer data on social networks.

Data Protection in Homeoffice

Safe working environment

- Use privacy filters
- Lock screen when away

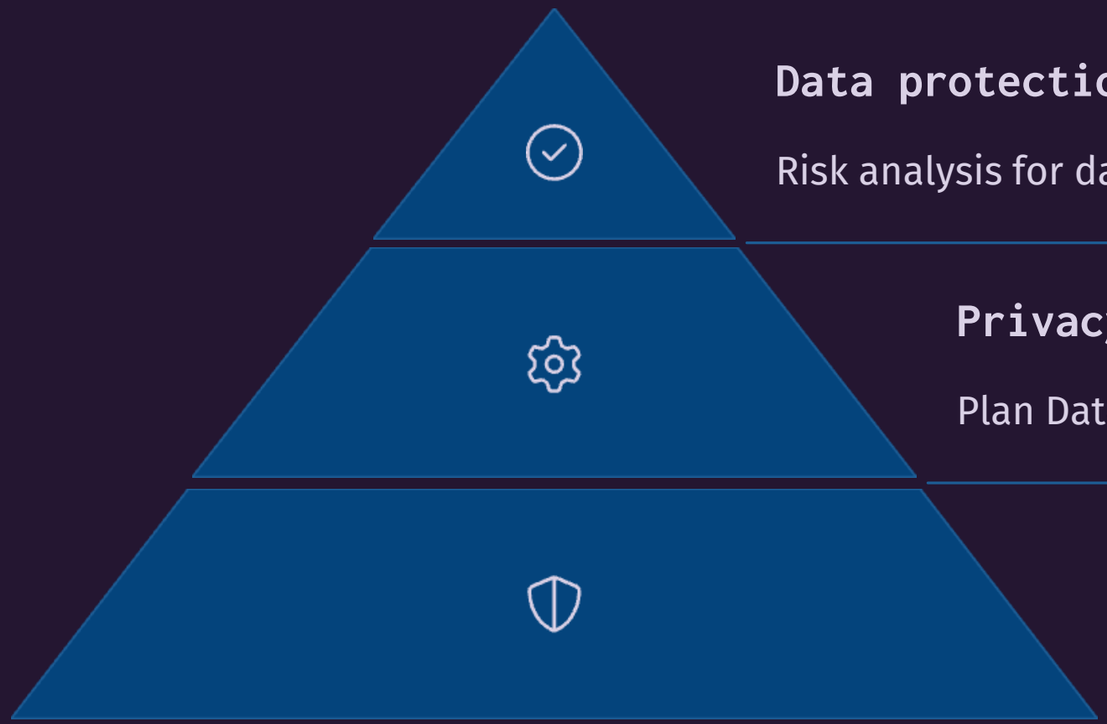
Access protection

- Safe WLAN-Connection
- Use VPN

Device Separation

- No private devices for work data

DSFA, Privacy by Design & Privacy by Default



Data protection impact assessment

Risk analysis for data processing

Privacy by Design

Plan Data Protection from the start

Privacy by Default

Data protection friendly basic settings

Data security & data breach

Data Security

Technical and organizational protective measures in accordance with Art. 32 GDPR.

- Encryption
- Access controls
- Regular checks

Data Breach

Breach of personal data protection.

- Unauthorized access
- Accidental loss
- Data theft

Reporting requirements

In the event of data breaches within 72 hours.

- To supervisory authority
- To those affected

PROTECTIT

Report immediately! The right way.

Recognize

Take suspected data protection violations seriously immediately.

Report

Immediately forward to DPC, DPO and management.

Documentation

Record who, what, when, where and how in detail

Data protection incidents: definition and examples

Loss

Lost laptops or smartphones with unencrypted customer data.

Theft

Targeted theft of data storage devices or phishing attacks on employees.

Unauthorized access

Hacker attacks on company databases or accidental data disclosure to unauthorized persons.

Data protection and artificial intelligence

Challenges and opportunities

A critical examination of the tension between AI innovations and data protection requirements.

What is Artificial Intelligence (AI?)

Weak vs. Strong AI

Specialized systems vs. human-like intelligence

Monitored Learning

Training with labeled data

Reinforcement learning

Learning through reward and punishment

Unsupervised learning

Independent pattern recognition in data

The challenges of data protection in AI

Data Collection

AI requires huge amounts of data for training.

Profiling

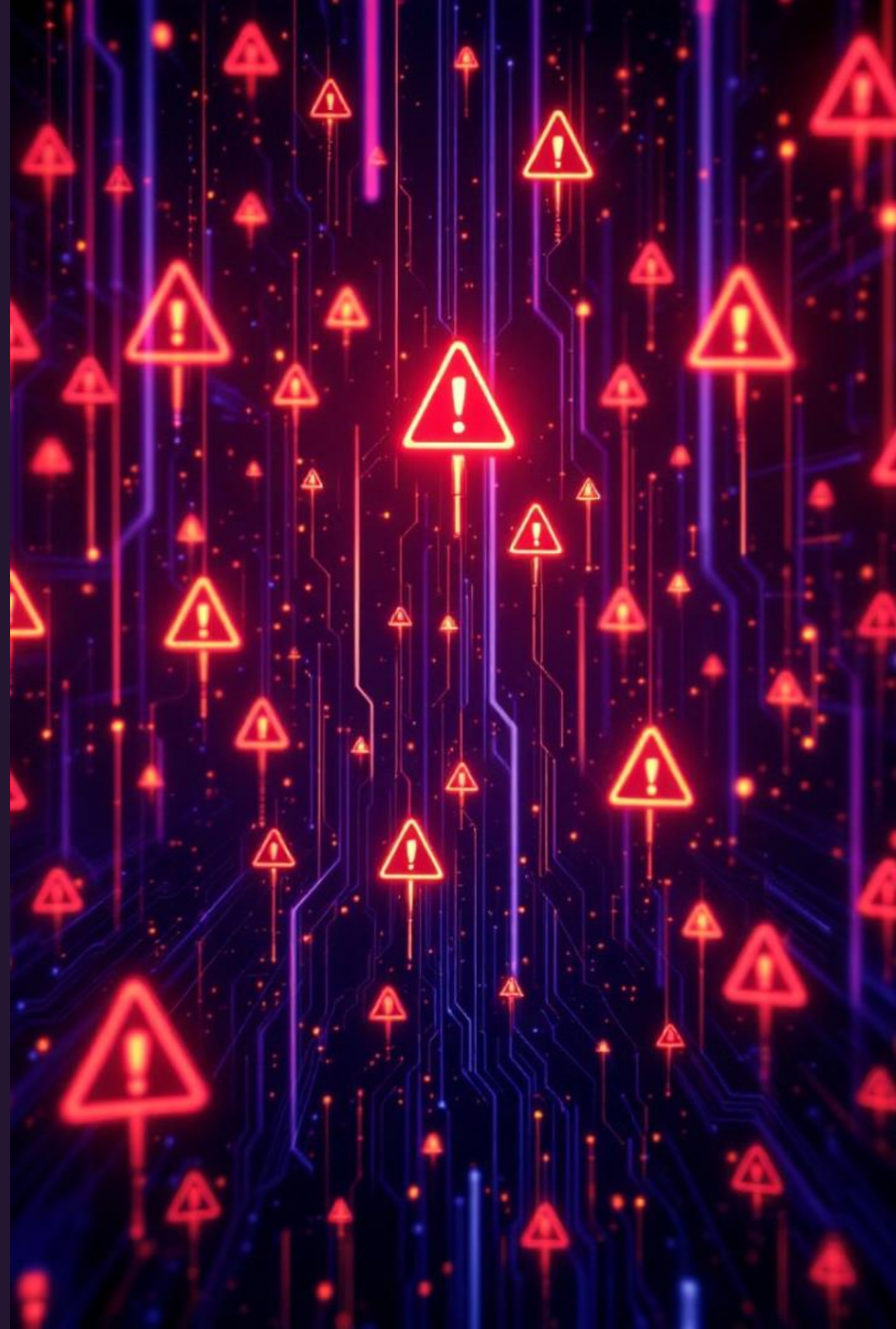
Risk of discrimination and surveillance

Transparency problems

"Black Box"-Systems are difficult to understand

Safety Risks

Protection against data leaks and manipulation



PROTECTIT

Opportunities of AI for data protection

Detecting violations

AI can automatically detect and report data breaches

Improved anonymization

AI-supported processes make personal data unrecognizable

Defense against cyber attacks

AI detects suspicious patterns and fends off attacks in real time.

Federated Learning

Data protection-friendly training without central data storage.

Best Practices for Data Protection using AI

Data protection impact assessment

Conduct risk assessment before deploying new AI systems.

Obtain consents

Ensure transparent information and voluntary consent of those affected.

Technical measures

Implement encryption and access controls

Continuous monitoring

Regular review of the effectiveness of all protective measures.

Case studies: Data protection and AI in practice

Successful applications

- Medical diagnosis with anonymize
- Smart traffic control without personal identification
- Fraud detection with privacy by design

Data breaches

- Face recognition scandals
- Unauthorized data use by voice assistants
- Discriminatory algorithms in lending

Conclusion and outlook for AI

89%

Consumer Concerns

Percentage of Germans with data protection concerns when using AI

60%

Growth Potential

Forecasted growth for privacy-compliant AI solutions

42%

Implementation Rate

Companies with data protection-compliant AI strategies

Data protection and AI don't have to be mutually exclusive. Ethical AI development requires integrated data protection concepts from the outset.

Data protection in practice

We've learned a lot. Remember: Your data is like your underwear.

Don´t show everyone

Be selective about who you grant access to

Change regularly

Update your passwords monthly

Keep well protected

Encryption is your best friend

JH

Or to put it another way

Confidentiality, Integrity, Availability

100%

Confidentiality

Access only for authorized persons with legitimate interests.

100%

Integrity

Protection against unauthorized changes or manipulation.

100%

Availability

Data is accessible at any time for authorized processes.

Next steps

Apply knowledge

Implementing data protection in everyday life

Ask and clear questions

Contact your DPO

Repeat regularly

Annual knowledge refresher

Your lifeline in the data protection ocean

Data protection Officer

Larissa Haug

E-Mail

l.haug@mhg-protectit.de

Phone

+49 7473 240940

Data Protection Assistant

Joachim Hittinger

E-Mail

j.Hittinger@mhg-protectit.de

Phone

+49 7473 240941

Please don´t forget the final test

Multiple-Choice-Test

Questions about the training content

Limit to consist 70%

If you fail you can repeat the test

Get Certificate

Automatic dispatch after passing the test