1

WHAT IS GDPR?

- General Data Protection Regulation.
- Standardization of data protection within the EU.

25

Deadline

May 25, 2018

2 WHO IS AFFECTED?

All organisations & companies worldwide that want to process or store data of natural persons (citizens) of the EU are affected.

3 FACTS AND FIGURES

Penalties

up to **20** million €

up to **4%** of annual global sales

Bills

archive for **10** years

IP adresses & pseudonymous **Cookies**

- Are personal data.

- Must be treated confidentially.

Personal data must be protected against unauthorized access by technical and organizational measures ("TOMs").

Data protection declaration

- Must be easy to understand.
- Has to published completely.

Checklist Data protection principles

✓ Legality

✓ Transparency (see information obligations Art. 13 and 14 GDPR)

✓ Legal obligations

Example: Archiving of invoices.

- ✓ Prohibition with reservation of permission (in case of processing of personal data).
- ✓ Earmarking
    - Data is used exclusively for a particular purpose, for which it was collected.
- ✓ Data minimisation
    - Data collection on stock prohibited. (Art. 5 Par. 1 lit. c GDPR)
- ✓ Integrity and trust

Data collection on stock

is prohibited

Privacy by Design

Data protection measures must already be included in the conceptual development of products and processes in accordance with the **state of the art**.

Privacy by Default

The default settings for devices or online platforms must be at the **highest level** of data protection.

Example: A newsletter checkbox must not be checked by default.

Data retention

☑ The user of the site must give his explicit consent

- No disadvantages in case of non-delivery.

- Consent must be time logged.
- Doubts always with the data processor.

Example: Closed user area on a website or shop registration.

Contract for order processing

Basis for the processing of personal data by service providers.

Data shall only be processed in accordance with the order and according to instructions.

Example: Web Hoster, Web Agency, ERP or CRM in the Cloud, Google, etc.

Checklist Contract for order processing

✓ Information about the client and contractor

✓ Categories of data processed

- ✓ Categories of processing of data subjects
- ✓ Purpose of processing
- ✓ Contractual obligations for compliance with instructions, approval of controls, commissioning of subcontractors only with consent, cooperation and information.
- ✓ Contract period
- ✓ Technical-organizational protective measures and other guarantees.

Example: Encryption of development or preview environments (staging).

- ✓ List of subcontractors

Example: Agency uses freelancer.

Data handling

Checklist

(Art. 6 GDPR)

- ✓ Consent of the natural person
- ✓ Fulfillment of the contract
- ✓ Legal obligations
- ✓ Protection of vital interests of people

✓ Legitimate Interest

Checklist Adherence to special rules

Children and minors (Art. 8 GDPR)

✓ Consider children's inexperience

✓ Age limit for effective consent of minors aged 16 and over.

✓ Up to 16 years of age - parental consent required.

Particularly sensitive data (Art. 9 GDPR)

✓ Explicit consent of the affected person.

✓ These include: Information on ethnicity, health, sexuality, religious or political views, biometrics or genetics.

Special rules for employees (§26 BDSG-Neu)

- ✓ Employee data protection
- ✓ Imbalance at the expense of employees
- ✓ Imbalance must be taken into account, for example, when assessing whether the legitimate interests of employers outweigh those of employees
- ✓ High standards for the consent and secret observation of employees

Video surveillance (§4 BDSG-Neu)

- ✓ Rules for video surveillance in public areas have been completely adopted.

Change of purpose (Art. 6 Par. 4 GDPR)

- ✓ A change of purpose is permitted if the new processing purpose is compatible with the old one, data is pseudonymised as far as possible and the persons concerned are not additionally burdened.

Checklist Transfer data to third countries

An adequate level of data protection has been determined. (Art. 45 GDPR).

- ✓ Decisions on adequacy
- ✓ US companies certified under the Privacy Shield Agreement

Where an adequate level of data protection has not been established, appropriate safeguards must be provided (Art. 46 GDPR).

- ✓ Internal Company Commitments
- ✓ Commission/supervisory authority standard data protection clauses
- ✓ Approved certification procedures

Exceptions were made for certain cases (Art. 49 GDPR)

- ✓ Consent of users
- ✓ Disclosure of data is required for the performance of the contract
- ✓ Prosecution of legal claims

Legitimate interest

- Users are interested in data protection.
- Website operators have economic interests.
- Weigh up opposing interests.

Online Marketing

- Analysis, optimization and economic advantages are legitimate interests that can be invoked when using the tools.
- **Profiling** is a legally anchored **risk indicator**.

Example: Motion profiles of users of an online shop.

Obligation to report

Data leaks

- Notification to the data protection authority. (Art. 33 GDPR)
- Is there a reportable data breach?
- Notification to affected persons. (Art. 34 GDPR)

Example: Customer data compromised in the context of a shop hack.

- Content of the message: All available information + name, company, address, responsible persons and their contact data.
- **72h of time**
- Notification via email

- ✓ Right of access (Art. 15 GDPR)
  - Request: Which data is stored about me?
  - Answer must be comprehensive (not only online shop, but also ERP, newsletter, etc.)
  - Attention: Authorization validation required.
- ✓ Right of rectification (Art. 16 GDPR)
  - Request: I would like to have my data corrected.
- ✓ Right to erasure and restrict the processing of data (Art. 17 GDPR)
- ✓ Right to be forgotten (Art. 17 GDPR)
- ✓ Right to data portability (Art. 20 GDPR)
  - Make the export of data possible early, e.g. as CSV file.
- ✓ Right to object (Art. 21 GDPR)
- ✓ Right of complaint to supervisory authorities

Updates

! Law since 2015

- Updates must be done **immediately.**
- Both software and hardware.
- Keeping technology up to date.

Documentation & verification obligations

Proof must be kept of data processing processes.

Purposes, type and scope and risk-reducing measures such as "Privacy by Design" must be documented and admissibility checked.

Tip: Create a data processing directory and document it comprehensively.

Checkliste When is the CEO liable?

- ✓ In the case of self-inflicted data protection violations.
- ✓ It is liable as a so-called "guarantor" for the fact that the members of the company adhere to the data protection law.
- ✓ Introduce data protection compliance in the company to avoid liability.
  - Responsible staff must be carefully selected, instructed and regularly monitored.
- ✓ Complete delegation of liability to one employee is not possible.
- ✓ Liability cannot be transferred completely to the data protection officer.

Tip: Insurance against loss, alteration or blocking of electronic data. Also demand such from your service providers.

Checklist Transition GDPR

- ✓ Check all data processing processes for admissibility.
- ✓ Create a procedure directory with an overview of all data processing processes.
- ✓ Verify that the requirements for the technical and organisational security of data subjects are met and, where appropriate, carry out a data impact assessment.
- ✓ Check whether a **data protection officer** needs to be appointed?
  - Companies with 10 employees and higher (§38 BDSG-Neu)
- ✓ Check whether data transfer processes are permissible and necessary order processing contracts are available.
- ✓ Examine whether a complaint management system is in place for cases of assertion of rights of the persons

concerned.

- ✓ Update Privacy Statement
- ✓ Sensitize employees, commit them to confidentiality, encourage them to comply with the **principles** of **Privacy by Design** and **Privacy by Default** and document all processes relevant to data protection law.
- ✓ Regularly monitor whether the data protection processes continue to comply with legal requirements.

This information graphic does not represent legal advice.

Copyright ® web-vision GmbH