

# JAHRESUNTERWEISUNG 2025

**Datenschutz**

Dezember 2024

Angela Bialke (Datenschutzbeauftragte)

# Inhalt

1. Einführung
2. Entwicklung des Datenschutzrechts
3. Abgrenzung der Begriffe
4. Pflichten im Umgang mit personenbezogenen Daten
5. Verstöße gegen die DS-GVO
6. Datenschutz in der EWN GmbH

Abbildungen aus / Inhalte teilweise basierend auf: „Datenschutzeinführung für Mitarbeiter und Führungskräfte Version 3.0“ von [www.dmc-datenschutz.de](http://www.dmc-datenschutz.de) und [www.datakontext.com](http://www.datakontext.com)

# EINFÜHRUNG

Worum geht es?

# Datenschutz ist Ihr Grundrecht

## In der EU

- Artikel 8 der EU-Grundrechtecharta: „Schutz personenbezogener Daten“

## In Deutschland

- Artikel 1 und 2 des Grundgesetzes



# ENTWICKLUNG DES DATENSCHUTZRECHTS

Datenschutz ist nichts neues...

# Datenschutz in der Geschichte

- **Schutz der Privatsphäre** in der Geschichte:
  - Ärztliche Schweigepflicht (Hippokratischer Eid, erstmals im 1. Jh. n. Chr. bezeugt)
  - Beichtgeheimnis (seit 1215 n. Chr.)
  - Postgeheimnis (seit dem 17. Jh.)
  - Steuergeheimnis (seit 1976)
- **1970 Hessen** erlässt das erste **Datenschutzgesetz** der Welt.
- **1977** Das Bundesdatenschutzgesetzes (**BDSG**) wird erlassen.

# Datenschutz in Deutschland

- **1983** Der Erste Senat des Bundesverfassungsgerichts fällt das sogenannte **Volkszählungsurteil**:

*„**Freie Entfaltung der Persönlichkeit** setzt unter den modernen Bedingungen der Datenverarbeitung den **Schutz** des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe **seiner persönlichen Daten** voraus.“*

Das Gericht erkannte die Gefahr des **Datenmissbrauchs** und sah damit das sogenannte „**Grundrecht auf informationelle Selbstbestimmung**“ und die nach Art. 2 Abs. 1 des Grundgesetzes garantierte **freie Entfaltung der Persönlichkeit** des Einzelnen als **gefährdet** an. Jeder Mensch soll grundsätzlich **selbst** über die Preisgabe und Verwendung seiner **persönlichen Daten bestimmen**.

- **1990** Novellierung des **BDSG**.

# Datenschutz in der EU

- **1995** Die „*Europäische Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*“ wird erlassen. Als Richtlinie muss sie in **nationales Recht umgesetzt** werden.
- **2001** Das **BDSG** wird **novelliert** und damit die Richtlinie von 1995 umgesetzt.
- **2014** Das Europäische Parlament legt einen **ersten Entwurf** der **Europäischen Datenschutzgrundverordnung (DS-GVO)** vor.
- **2016** Am 24. Mai **tritt die** EU DS-GVO in Kraft - mit **zweijähriger Übergangszeit** zur Umsetzung.
- **2018 Novellierung** des **BDSG** zur Anpassung an die EU DS-GVO **tritt in Kraft**.

# Datenschutz aktuell

- **2021** Das **TTDSG** tritt am 01. Dezember „zum Datenschutz und Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ parallel mit einer neuen Fassung des **TKG** (Telekommunikationsgesetz) in Kraft
- **2024** EU Verordnung **Digital Services Act** zu einheitlichen Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte
- **2024** das Digitale-Dienste-Gesetz (**DDG**) tritt in Kraft:
  - ergänzt den Digital Services Act,
  - löst das Telemediengesetz (TMG) und das Netzwerkdurchsetzungsgesetz (NetzDG) ab und
  - benennt es das bisherige TTDSG in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (**TDDDG**)

# Datenschutz international

- Austausch grundsätzlich zulässig<sup>\*)</sup>:
  - innerhalb der EU,
  - innerhalb des Europäischen Wirtschaftsraums
  - mit Drittstaaten, zu denen ein Angemessenheitsbeschluss
- Für sonstige Drittstaaten gilt<sup>\*)</sup>:
  - Nachweis geeigneter Garantien durch den Dienstleister (bspw. Standardvertragsklauseln)
  - Zusammenarbeit mit **US-Unternehmen/US-Dienstleistern**<sup>\*)</sup>: Seit 2023 freiwillige Zertifizierung nach dem **EU-U.S. Data Privacy Framework** möglich [<https://www.dataprivacyframework.gov/s/participant-search>]

<sup>\*)</sup> immer unter der Voraussetzung, dass die gesetzlichen Bestimmungen eingehalten werden

# Die DS-GVO nervt!



Erzaehlmirnix; 30. Tätigkeitsbericht des BfDI; 2021

Werbeeinnahmen am Beispiel:

Alphabet (das Mutterunternehmen von Google: 76 % des Umsatzes durch Werbung, Meta, das Mutterunternehmen von Facebook und Instagram, 97 %. Online wird individuelles Verhalten für Werbezwecke detailliert verfolgt, um Werbesegmente und Profile zu erstellen. Diese dienen Verhaltensvorhersagen und personalisierter Werbeplatzierung.

Wer digitale Werbeflächen bereitstellt, lässt anhand detaillierter Informationen das Verhalten einzelner Nutzer:innen abschätzen, um Werbetreibenden eine passgenaue Vermarktung anzubieten.

# Was bringt die DS-GVO wirklich?

- Die EU-Verordnung soll sicherstellen, dass **EU-Bürger datenschutzrechtlich geschützt** sind und gleichzeitig der **freie Datenverkehr innerhalb des EU-Binnenmarkts gewährleistet** wird.
- Verbraucher erhalten mehr Rechte.
- Für Unternehmen bedeutet das **strengere Auflagen und mehr Pflichten**.
- Alle Anforderungen haben eines gemeinsam: Unternehmen benötigen einen genauen **Überblick über** die von ihnen gespeicherten **Daten** und verwendeten **Verfahren**.
- Es gilt das **Marktortprinzip**: Die DS-GVO ist für internationale Unternehmen verbindlich, wenn sie ihre Dienste in EU-Staaten anbieten.

# DATENSCHUTZ IM ÜBERBLICK

## Abgrenzung der Begriffe

# „Betroffene“ und „Verantwortliche“

**Betroffene sind Personen, deren Daten verarbeitet werden**

- Bspw. aktive, passive und ehemalige Mitarbeiter, ANÜ, Auszubildende, Kunden oder Ansprechpartner der EWN GmbH
- KEINE juristischen Personen, Vereine, Verbände etc.



**Verantwortliche legen die Zwecke und Mittel der Datenverarbeitung fest**

- Natürliche oder juristische Personen, Behörden, Einrichtungen oder Stellen, die allein oder gemeinsam entscheiden
- Bspw. die EWN GmbH
- (Mit-)Verantwortung tragen alle Mitarbeiter, insbesondere die Führungskräfte

# Aufsicht und Überwachung

**Zuständig für die Einhaltung des innerbetrieblichen Datenschutzes sind:**

**Angela Bialke**

Datenschutzbeauftragte  
Telefon +49 38354 4-5307

**Peter Huyoff**

Stellv. Datenschutzbeauftragter  
Telefon +49 38354 4-3738

[datenschutz@ewn-gmbh.de](mailto:datenschutz@ewn-gmbh.de)

[https://intranet.intern/  
beauftragte/datenschutzbeauftragte](https://intranet.intern/beauftragte/datenschutzbeauftragte)

**Zuständige Aufsichtsbehörde für die EWN GmbH als Bundesunternehmen:**

**BfDI**

Der Bundesbeauftragte für den Datenschutz  
und die Informationsfreiheit

Graurheindorfer Straße 153  
53117 Bonn  
Telefon +49 228 997799-0

[poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

<https://www.bfdi.bund.de/>

# Was sind „personenbezogene Daten“?

Alle Angaben, die sich auf eine identifizierte oder identifizierbare Person beziehen, beispielsweise:



- Namen
- Adresse
- Geburtsdatum
- Telefonnummer
- Vermögen / Besitz

- Gehalt
- Fotos
- Personalnummer
- Benutzerkennung

- Arbeitsverhalten / Arbeitsergebnisse
- Maschinenbezogene Nutzungsdaten



Besonders sensible Daten sind besondere Kategorien personenbezogener Daten:

- Genetische und Gesundheitsdaten
- Biometrische Daten (bspw. Fingerabdrücke)
- Gewerkschaftszugehörigkeit
- Rassistische oder ethnische Herkunft
- Politische, Religiöse oder weltanschauliche Überzeugung
- Sexualleben / sexuelle Orientierung

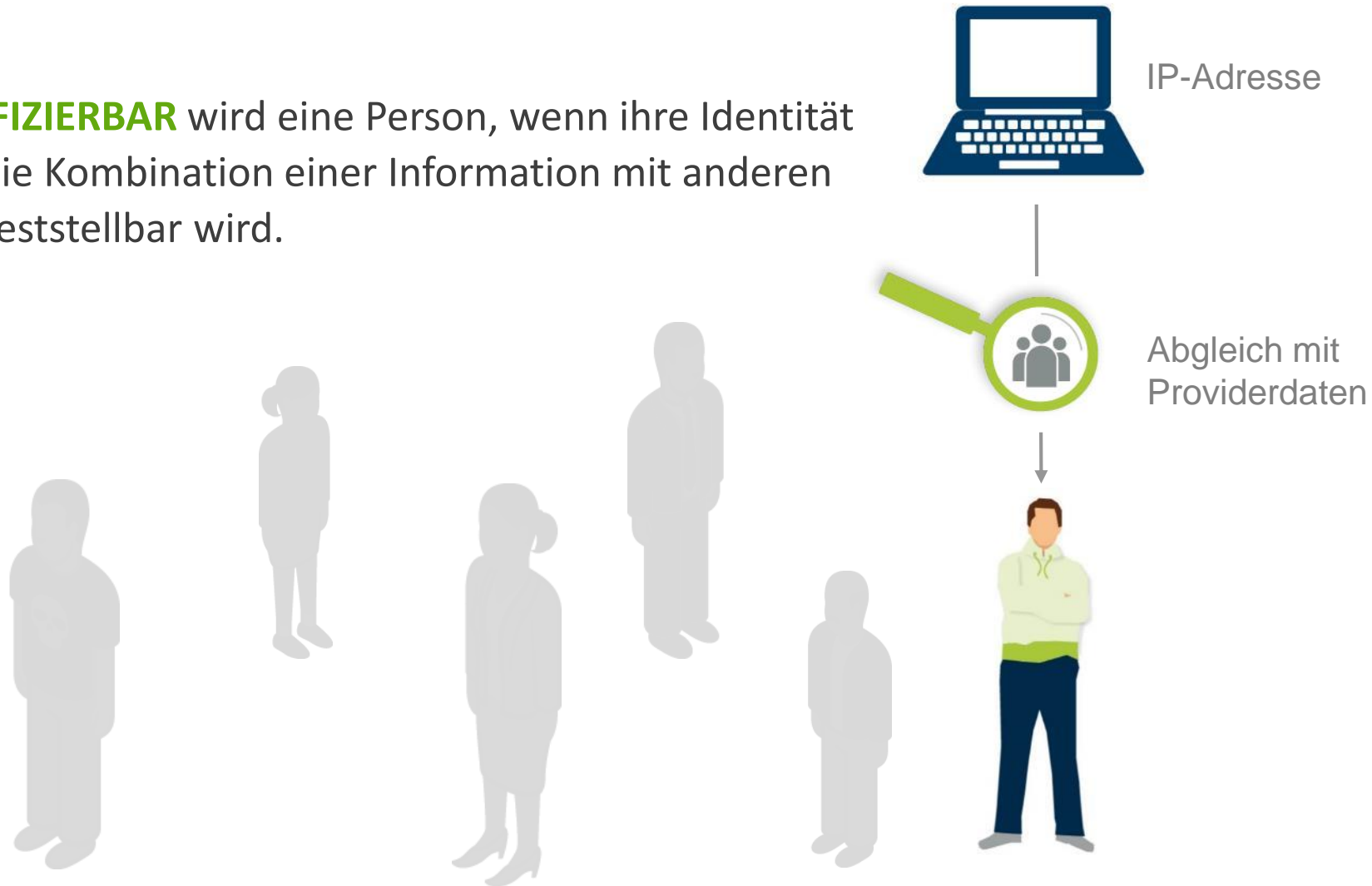
# Was ist ein „identifizierte Person“?

- **IDENTIFIZIERT** ist eine Person, wenn sich ihre Identität direkt aus den bekannten Informationen oder einer Teilmenge davon ergibt:



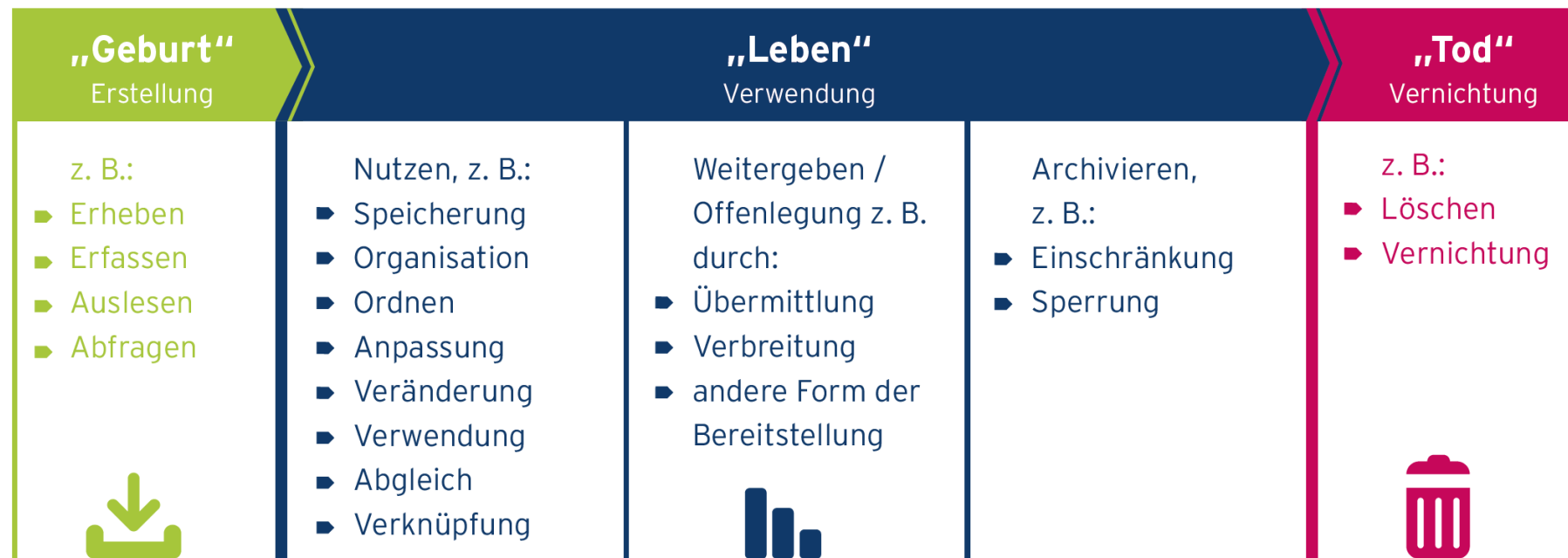
# Was ist ein „identifizierbare Person“?

- **IDENTIFIZIERBAR** wird eine Person, wenn ihre Identität durch die Kombination einer Information mit anderen Daten feststellbar wird.

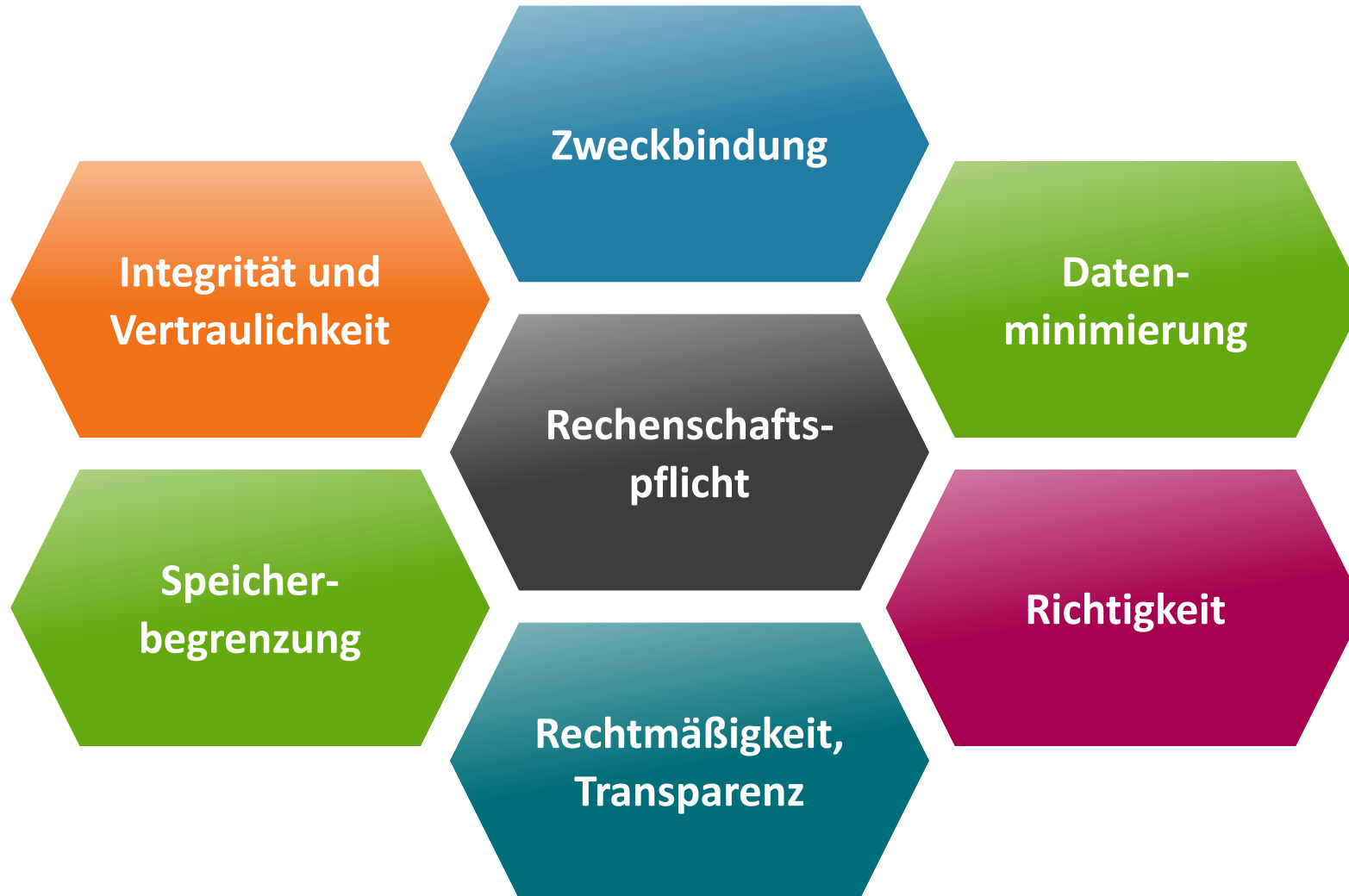


# Was bedeutet „Verarbeitung“ personenbezogener Daten?

- Unter der Verarbeitung wird die Erstellung, die Verwendung und die Vernichtung der personenbezogenen Daten verstanden („Lebenslauf“ der Daten)
- Der Anwendungsbereich des Datenschutzes umfasst jede Verarbeitung von personenbezogenen Daten, sowohl in digitaler als auch in analoger Form.



# Bei der Verarbeitung sind „Grundsätze“ einzuhalten



# Grundsätze: „Rechtmäßigkeit“

## Verbot mit Erlaubnisvorbehalt

Das Datenschutzrecht verbietet grundsätzlich den Umgang mit personenbezogenen Daten, erlaubt diesen aber unter bestimmten Voraussetzungen.

Die Datenverarbeitung ist somit zulässig, wenn sie erlaubt wird. Beispielsweise ...

- ... durch das **Datenschutzrecht selbst**.

Beispiel: die Verarbeitung dient dem Zweck der Erfüllung eines Vertrags mit dem Betroffenen (Artikel)



- ... durch eine **andere Rechtsvorschrift**.

Beispiel: Steuerrecht, Telekommunikationsgesetz, Telemediengesetz, StrlSchV



- ... durch die **Einwilligung** des Betroffenen.

Beispiel: Einverständniserklärung zur Datennutzung



# Grundsätze: „Transparenz“ - „Zweckbindung“

## Transparenz

- Die Verarbeitung muss für betroffene Personen nachvollziehbar sein.
- Dazu müssen die Personen in leicht verständlicher Weise über Risiken, Vorschriften und Rechte informiert werden.

## Zweckbindung der Daten

- Personenbezogene Daten dürfen nur für im Vorfeld festgelegte, eindeutige und legitime Zwecke verarbeitet werden.

# Grundsätze: „Datenminimierung“ - „Speicherbegrenzung“

## Datenminimierung

- Es dürfen nur die Daten erhoben werden, die notwendig sind, um den Zweck zu erfüllen.

## Speicherbegrenzung

- Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- Es müssen Löschfristen festgelegt und geeignete Maßnahmen für Löschroutinen implementiert werden. Die Löschung muss dokumentiert werden.

# Grundsätze: „Richtigkeit“ - „Integrität“ - „Vertraulichkeit“

## Richtigkeit

- Die personenbezogenen Daten müssen sachlich richtig und auf dem aktuellen Stand sein.
- Zur Sicherstellung dieser Forderung müssen entsprechende Maßnahmen implementiert werden.

## Integrität und Vertraulichkeit

- Personenbezogene Daten müssen durch technische und organisatorische Maßnahmen (TOM) vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung oder Schädigung geschützt werden.

# Grundsätze: „Rechenschaftspflicht“

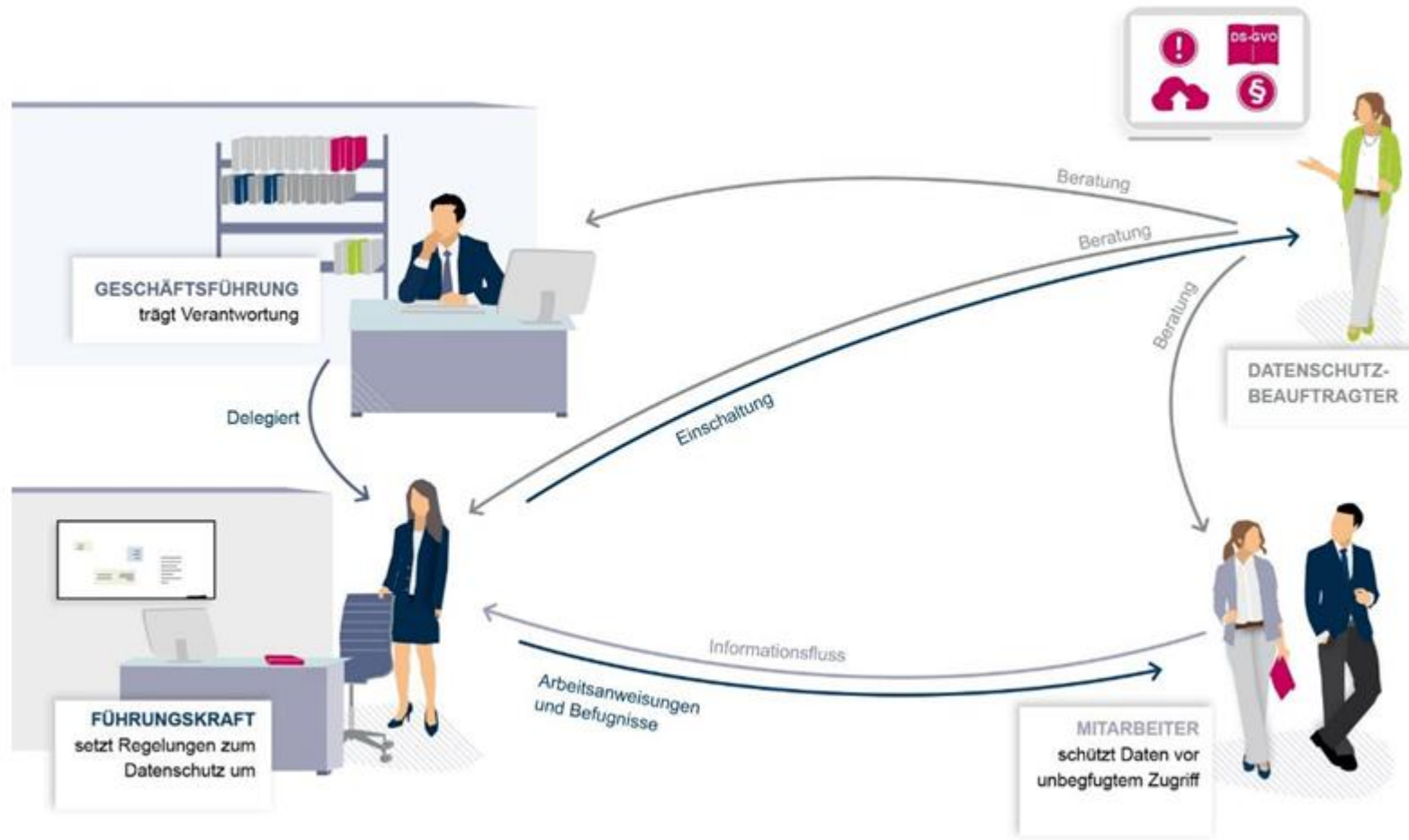
## Rechenschaftspflicht

- Der Verantwortliche muss u. a. ...
  - ... nachweisen, dass Gesetze geachtet werden.
  - ... (auf Anfrage) nachweisen, welche technischen und organisatorischen Maßnahmen ergriffen wurden und dass diese wirksam sind.
  - ... angemessene Dokumentation darüber führen, wie die Grundsätze der DSGVO eingehalten werden.
  - ... Dokumentation der Prozesse und Verfahren zur frühzeitigen Reaktion auf Datenschutzverletzungen
  - ... die Einbindung eines Datenschutzbeauftragten in die organisatorische Planung und Betriebsabläufe nachweisen

# IHRE PFLICHTEN

Was müssen Sie im Umgang mit personenbezogenen Daten beachten?

# Datenschutz ist Aufgabe des gesamten Unternehmens!



# Pflichten der Führungskräfte



- **Umsetzung** der rechtlichen und internen Regelungen zum Datenschutz und **Kontrolle** der Einhaltung
- **Schaffung der Voraussetzungen** für einen ausreichenden Schutz von personenbezogenen Daten - Zuständigkeiten regeln, Berechtigungskonzepte erstellen, pflegen.
- **Sensibilisierung der Mitarbeiter** für die besondere Bedeutung des Datenschutzes
- **Unterstützung der Mitarbeiter** bei der Einhaltung des Datenschutzes
- Meldung von **Verarbeitungstätigkeiten**
- **Einbindung des Datenschutzbeauftragten** insbesondere bei neuen oder geänderten Verarbeitungstätigkeiten

# Pflichten aller Mitarbeitenden



- **Einhaltung der** gesetzlichen und internen **Regelungen**
- **Schutz** personenbezogener Daten **vor unbefugtem Zugriff** und Vorsorge dafür, dass sie nicht in falsche Hände gelangen
- Der **Umgang** mit personenbezogenen Daten darf nur zur **Aufgabenerfüllung** nach Weisungen des Arbeitgebers erfolgen
- **Führungskraft und / oder Datenschutzbeauftragte über** Missbrauch, Verlust oder Manipulation informieren
- Über die **Informationen** und personenbezogenen **Daten** ist – auch außerhalb des Arbeitsverhältnisses – **Vertraulichkeit** zu wahren

# Besondere Verantwortung: Führungskräfte, Sekretariate, Assistenzen, Personalerinnen und Personaler

## „Aus großer Kraft folgt große Verantwortung“

- Das gilt nicht nur für Spiderman sondern auch für Führungskräfte, Sekretariate, Assistenzen und Mitarbeitende im Personalbereich.
  - Diese Berufsgruppen haben umfangreiche Befugnisse
  - und durch ihre Tätigkeiten besonders weitreichenden Zugang zu teils sensiblen Daten, seien es private Daten zu Hochzeiten, Scheidungen, Schwangerschaften oder Krankheiten aber auch dienstliche, hochpersönliche Angelegenheiten, wie Mitarbeitergespräche oder Abmahnungen laufen über ihren Tisch.
- ! *Von Mitarbeiterinnen und Mitarbeitern in diesen Positionen wird ein hohes Maß an verantwortungsbewussten Umgang mit den ihnen anvertrauten Informationen gefordert – im Zweifelsfall machen sie sich persönlich haftbar, wenn Informationen unerlaubt weiter gegeben werden.*

# Die Rechte der Betroffenen

- Diese Rechte muss die EWN gegenüber Beschäftigten, Kunden und weiteren Betroffenen gewährleisten:



# Auskunftsrecht und Informationspflicht



## Betroffener wird insb. informiert über:

- Daten bzw. Datenkategorien
- Zwecke und Rechtsgrundlage
- Berechtigte Interessen im Falle einer Interessenabwägung
- Empfänger, inkl. ggf. Drittländer
- Dauer der Speicherung
- Betroffenenrechte
- Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten

## Wenn Betroffene ihre Rechte geltend machen:

- Nehmen Sie den Wunsch auf.
- Versuchen Sie zu ergründen, was der Betroffene tatsächlich möchte.
- Geben Sie den Wunsch unverzüglich an die betrieblich zur Bearbeitung vorgesehenen Stellen (in der Regel zunächst KP) weiter.

# Meldung von „Verarbeitungstätigkeiten“

- Verantwortliche müssen ein Verzeichnis aller Verarbeitungstätigkeiten führen.
- Als Verarbeitungstätigkeit sind dabei alle Verarbeitungen personenbezogener Daten, einschließlich Papierunterlagen zu verstehen.
- Alle Verarbeitungstätigkeiten sind der Datenschutzbeauftragten mittels des dafür vorgesehenen Formulars zu melden.
- Die Meldung kann um projekt- / prozessinterne Dokumentation ergänzt werden, um Mehrarbeit zu vermeiden.

**1. Grundsätzliche Angaben zur Verarbeitungstätigkeit**

Organisationseinheit:
Verantwortliche Führungskraft:
Anspruchspartner:
Telefon-Nummer:
Name u. Anschrift des Auftragnehmers, wenn im Rahmen dieser Verarbeitungstätigkeit eine Auftragsverarbeitung nach Art. 28 DS-GVO (Hinweis Nr. 5) erfolgt:
Vertrags-Nummer:
Name u. Anschrift des Auftragnehmers, wenn im Rahmen dieser Verarbeitungstätigkeit eine Auftragsverarbeitung nach Art. 28 DS-GVO (Hinweis Nr. 5) erfolgt:
Vertrags-Nummer:
Name u. Anschrift des Auftragnehmers, wenn im Rahmen dieser Verarbeitungstätigkeit eine Auftragsverarbeitung nach Art. 28 DS-GVO (Hinweis Nr. 5) erfolgt:
Vertrags-Nummer:

**Erfassung einer personenbezogenen Verarbeitungstätigkeit**

**Anmerkungen:**  
Wenn der Platz dieses Formulars nicht ausreicht, fügen Sie bitte zusätzliche Anlagen bei. Das nächste Formularfeld wird jeweils mit der Tabulator-Taste angesprungen. Für die Erläuterungen zu den Hinweisen öffnen Sie bitte die Datei „Erläuterungen.pdf“. Die Artikel der DS-GVO und die §§ des BDSG neu finden Sie unter: <https://dsrvo-gesetz.de/>. Nach der Bearbeitung bitte an datenschutz@ewn-gmbh.de senden.

**Nur auszufüllen, wenn personenbezogene Daten (Hinweis 1) verarbeitet werden!**

Datum: 01.01.2019

Ausfüllende Person:

(Haupt)Abteilung:

Telefonnummer:

Bezeichnung der Verarbeitung (Hinweis Nr. 2):

Übergeordneter Geschäftsprozess:

Beginn der Verarbeitung (Hinweis Nr. 3): 01.01.2019

Neue Verarbeitung

Änderung bestehende Verarbeitung

Abmeldung bestehende Verarbeitung (Hinweis Nr. 4)

Der Datenbestand wird gelöscht.

Es ist geplant, den Datenbestand in die Verarbeitung zu überführen.

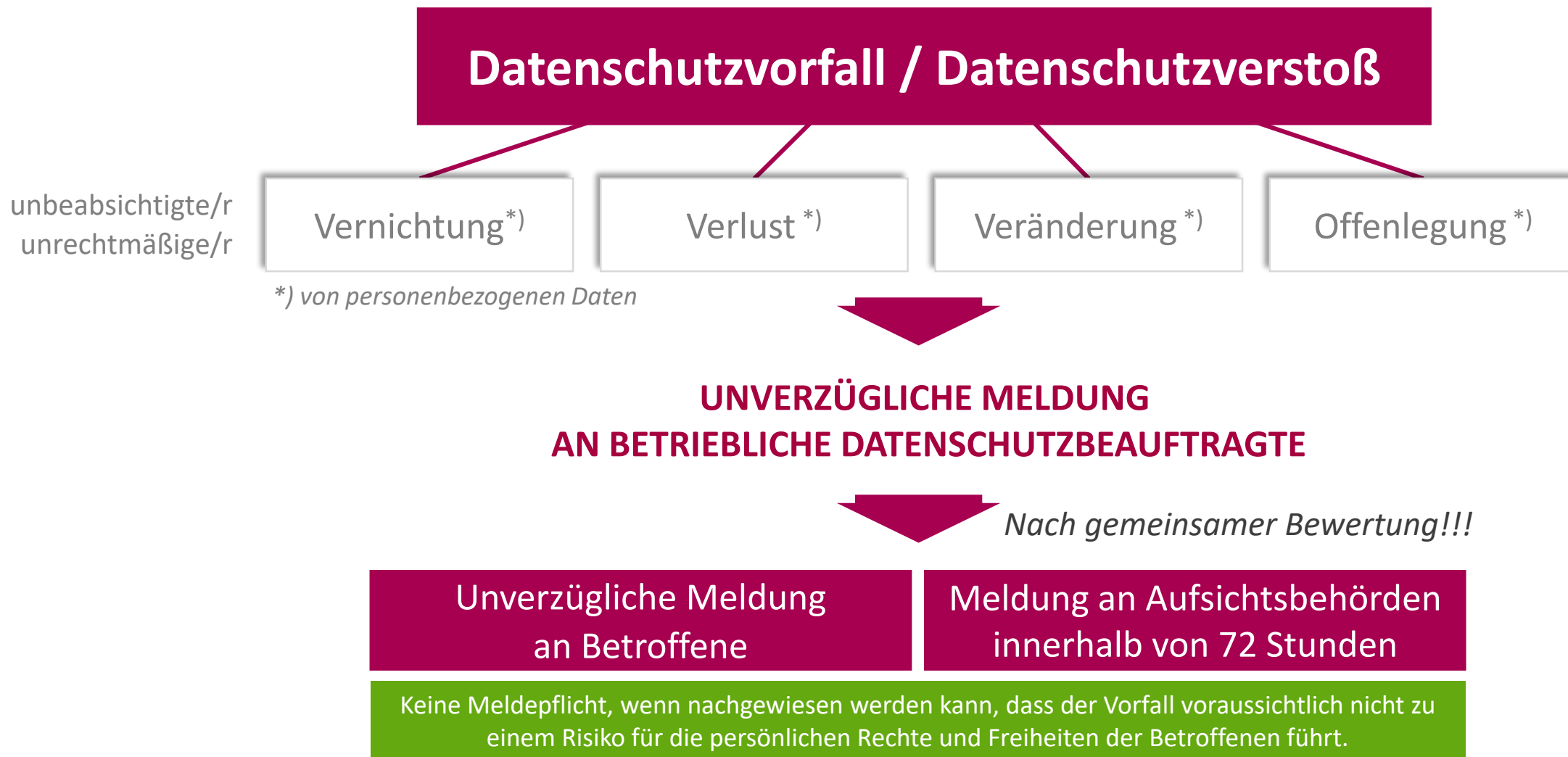
Seite 1 von 12

[https://intranet.intern/ileadadmin/Beauftragte/Datenschutzbeauftragte/Verarbeitungsmeldung/EWN\\_Organisationseinheit\\_Verarbeitungstaetigkeit\\_UJMMMTT\\_standz1.10.22.docx](https://intranet.intern/ileadadmin/Beauftragte/Datenschutzbeauftragte/Verarbeitungsmeldung/EWN_Organisationseinheit_Verarbeitungstaetigkeit_UJMMMTT_standz1.10.22.docx)

# VERSTÖßE GEGEN DIE DS-GVO

Mit welchen Sanktionen müssen Sie rechnen?

# Umgang mit „Pannen“



# Verstöße gegen die DS-GVO



Das **Unternehmen** hat die Datenschutzverantwortung!

In Fällen individuellen Fehlverhaltens können **Beschäftigte** zur Rechenschaft gezogen werden.

# Gemeldete Datenpannen - Statistik

- Häufigsten Kategorien von meldepflichtigen Datenpannen<sup>1)</sup>
  - (Unbeabsichtigte) Übermittlung von personenbezogenen Daten an falsch(n) Empfänger
  - Offene E-Mail-Verteiler (offenbaren unerlaubt E-Mail-Adressen)
  - Cyberkriminalität, insbesondere Verschlüsselung und Abgreifen personenbezogener Daten
  - Verlust von Unterlagen auf dem Postweg
  - Einbrüche / Diebstähle

1) Stand 2021; Erhebung des Datenschutzbeauftragten Sachsen

# Mögliche Sanktionen gegenüber dem Unternehmen



## RECHTSWEGE

- Beschwerde bei Aufsichtsbehörde
- Gerichtsverfahren gegen Aufsichtsbehörde
- Gerichtsverfahren gegen Verantwortlichen/ Auftragsverarbeiter



## VERTRETUNG

- Vertretung des Betroffenen durch einen Verband
- Verbandsklagerecht



## SANKTIONEN

- Schadensersatz, auch bei immateriellen Schäden
- **Bußgeld** bis zu 20.000.000 € oder 4% des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist
- Strafzahlungen

# Mögliche Sanktionen gegenüber Beschäftigten



# Haftung als Privatperson – Beispiele:

- Der Bußgeldempfänger hatte einen tätlichen Angriff auf einen Betroffenen gefilmt und die Aufnahme anschließend in einer WhatsApp-Gruppe mit zwölf Mitgliedern verbreitet: 2.000 EUR \*)
- Der Bußgeldempfänger hatte ein Video auf der Social-Media-Plattform Twitter gepostet. In der Aufnahme war zu sehen, wie eine Frau von einem Mann überfallen wird und wie ein Minderjähriger versucht, die Situation zu entschärfen: 6.000, ursprgl. 10.000EUR\*)
- Polizeibeamter hat die polizeilichen Datenbanken genutzt, um eine Zufallsbekanntschaft zu ermitteln: 1.400 EUR \*\*)

\*) <https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/>

\*\*\*) <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/>

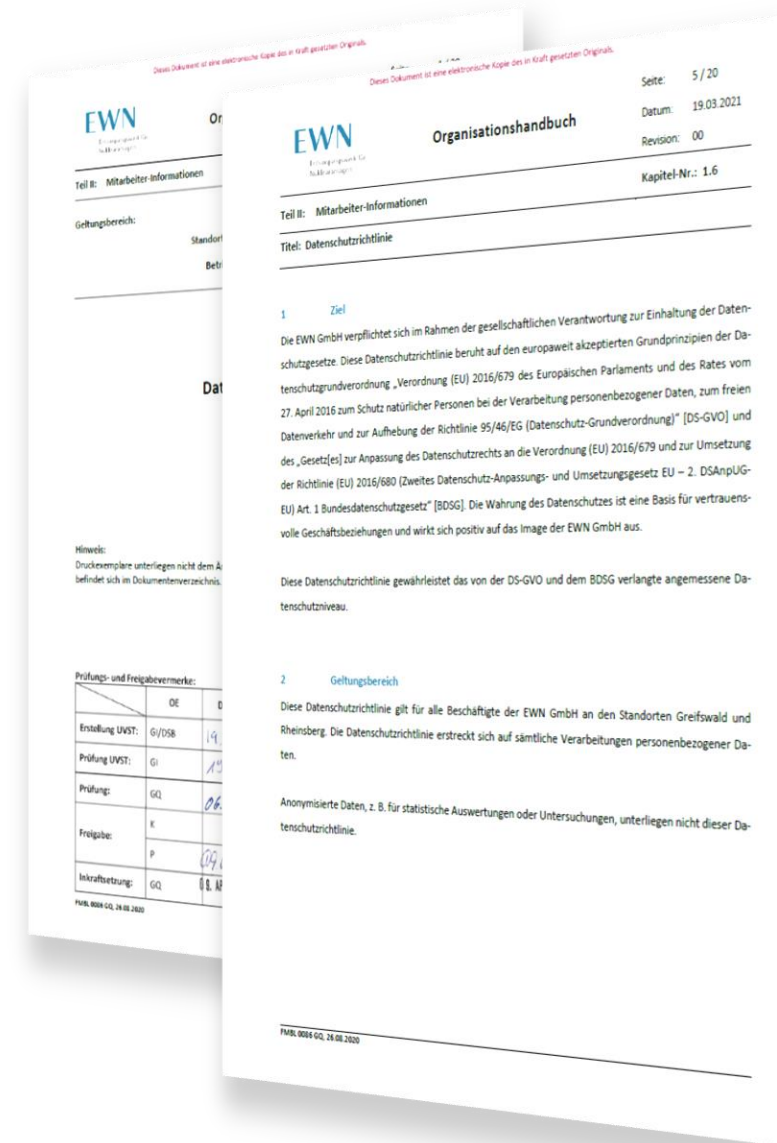
# DATENSCHUTZ IN DER EWN

## Alltag, Richtlinie und Beauftragte

# Datenschutzrichtlinie der EWN

*„Diese Datenschutzrichtlinie gilt für alle Beschäftigte der EWN GmbH an den Standorten Greifswald und Rheinsberg. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten.“*


- Sie ist Bestandteil des Organisationshandbuches OHB II/1.6



# Datenschutz im Alltag (1/2)

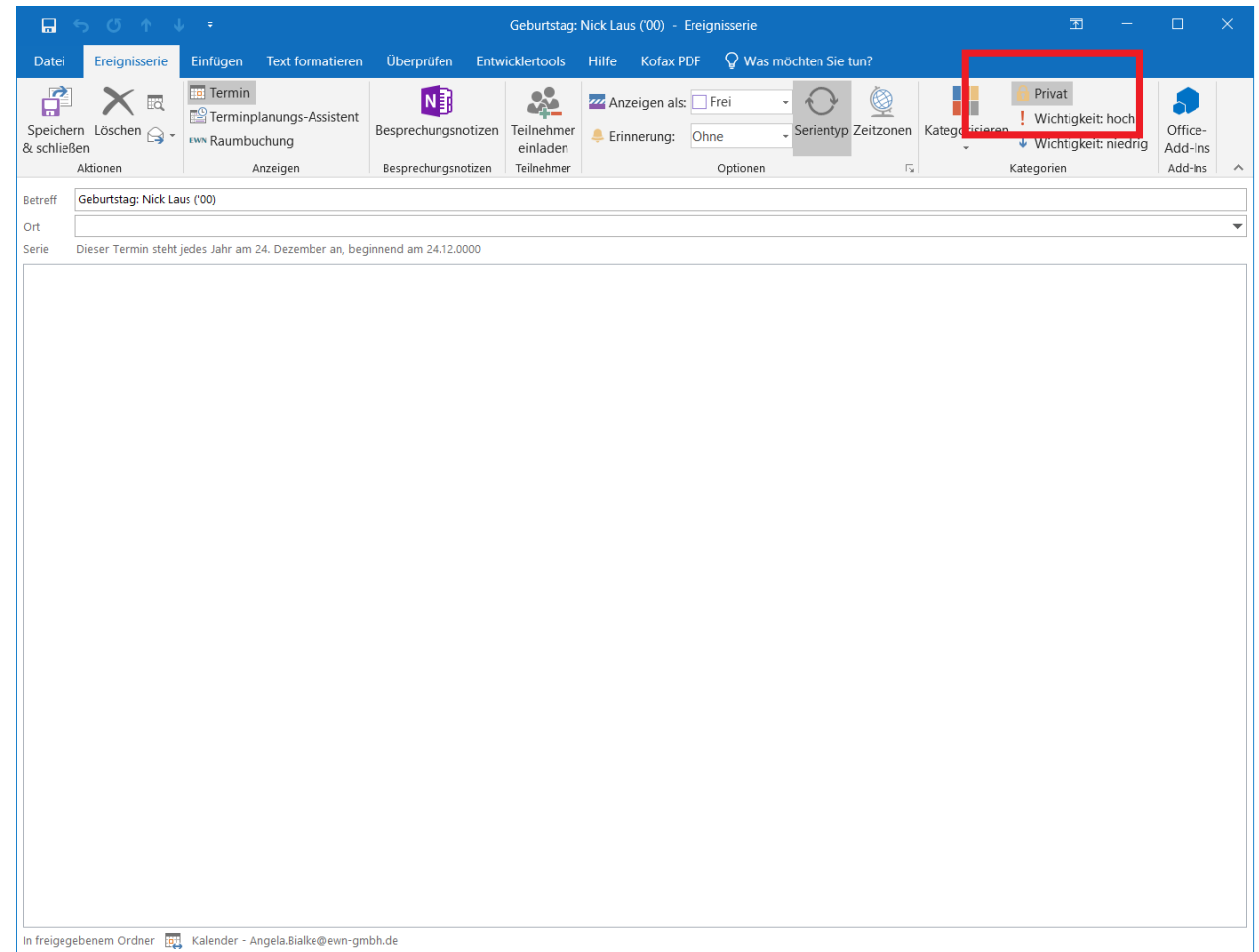
- "Harmlose" oder "freie" Daten gibt es nicht. Sobald die Daten personenbezogen sind, müssen die Regelungen des Datenschutzes beachtet werden. Das gilt auch für öffentlich zugängliche Daten aus dem Telefonbuch oder sozialen Medien.
- Es dürfen nur die Daten erhoben und verarbeitet werden, die zur Aufgabenerfüllung notwendig sind.
- Über die personenbezogenen Daten ist – insbesondere außerhalb des Arbeitsverhältnisses – Vertraulichkeit zu wahren.
- Beschäftigte dürfen personenbezogene Daten, die ihnen im Rahmen ihrer Tätigkeit zu Kenntnis kommen, nicht für private oder eigene wirtschaftliche Zwecke nutzen, an Unbefugte weitergeben oder diesen zugänglich machen.

# Datenschutz im Alltag (1/2)

- Besondere Sorgfalt gilt auch für die Nutzung privater Informationen von Mitarbeitern: Fragen Sie Ihre Kollegen um Erlaubnis, BEVOR Sie private Telefonnummern, E-Mail-Adressen oder Messenger-IDs an andere Kollegen weitergeben oder für Gruppenaktivitäten verwenden.
- Besondere Sorgfalt gilt im Umgang mit vertraulichen/persönlichen Unterlagen von Kollegen oder Bewerbern: Lassen Sie die Daten nie, auch nicht für den Gang zur Toilette oder zum Kopierer unverschlossen in Ihrem Büro liegen.  
! Sperren Sie bewusst den Bildschirm (Win  + L).

# Kalender/Outlook

- Jubiläen (Geburtstage, Jahrestage...) von Kollegen, Geschäftspartnern ... dürfen **nicht** offen einsehbar im Wand-/Tischkalender stehen.
- Jubiläumstermine in Outlook IMMER als „privat“ markieren (siehe rechts)
- Berücksichtigen Sie bei Terminen mit sensiblen Themen, für wen Ihr Kalender frei gegeben ist und seien Sie entsprechend umsichtig mit Details.



# Informationssicherheit im Alltag (1/2)

- Beachten Sie Aktualisierungen der Regelwerke der EWN.
- Geben Sie unbefugt keine Informationen an Dritte (Polizei, Sozialamt, Krankenkasse, Unbekannte etc.) weiter.  
! Bestehen Sie auf eine schriftliche Anfrage und die Nennung der Rechtsgrundlage!
- Verwehren Sie Unbefugten die Einsicht in Unterlagen/Kenntnis über die Informationen - das gilt für unbefugte Mitarbeitende und Externe gleichermaßen!
- Achten Sie besonders auf die Wahrung der Vertraulichkeit beim Einsatz mobiler Geräte wie Smartphones, Notebooks oder Tablets! Dies gilt bspw. auf Bahnfahrten: lassen Sie die Geräte niemals unbeaufsichtigt. Lassen Sie keine Mitreisenden auf den Bildschirm blicken.

## Informationssicherheit im Alltag (2/2)

- Clean-Desk-Prinzip: Halten Sie Ihren Schreibtisch aufgeräumt.
- Verwahren Sie Daten, Datenträger und Ausdrücke stets sicher, bspw. in verschlossenen Schränken – insbesondere bei der mobilen Arbeit.
- Schließen Sie das Büro ab, wenn sich für längere Zeit (bspw. Termine, Pausen) niemand darin befindet.
- Versenden oder transportieren Sie physische Unterlagen nur in verschlossenen Umschlägen oder Behältern.

# Daten und Datenträger

- Für alle Mitarbeitenden gilt OHB<sup>1)</sup> Teil III Kapitel 7.1

## „Organisation des Datenverarbeitungsprozesses“:

- Unternehmenseigene Daten dürfen nicht auf privaten Computern bearbeitet oder gespeichert werden.
- Private Daten dürfen nicht auf Unternehmenseigenen Computern bearbeitet oder gespeichert werden.
- Private Technik ist nicht in der EWN einzusetzen
  - Ausnahmen sind schriftlich durch die zuständige Abteilungsleitung und die IT-Abteilung zu regeln
- Datenträger (USB-Sticks...) sind einer Virenprüfung zu unterziehen.

1) Organisationshandbuch

# Mobile Arbeit

- Für alle Mitarbeitenden gilt die Gesamtbetriebsvereinbarung 01/2022<sup>1)</sup>

## „Mobile Arbeit“:

- Daten sind so zu sichern, dass Dritte (bspw. Familienmitglieder aber auch Haustiere) keinen Zugriff erhalten.
- Die Mitnahme papierbasierter Unterlagen (insbesondere VS-NfD, Personal- und Patientenakten, BEM-Unterlagen, Betriebsratsprotokolle) ist nicht gestattet.
- ! Bestehen Zweifel daran, ob bestimmte Unterlagen mit sensiblen Daten aus dem Unternehmen an den alternativen Arbeitsort mitgenommen werden dürfen, ist vorher die Zustimmung der Abteilungsleitung einzuholen.
- Für eine sachgemäße Vernichtung von Unterlagen ist Sorge zu tragen.
- ! ausschließlich Shredder oder bereit gestellte Container im Unternehmen

1) <https://intranet.intern/personal/betriebsvereinbarungen>

# Internet und E-Mail

- Für alle Mitarbeitenden gilt die Gesamtbetriebsvereinbarung 01/2017<sup>1)</sup>

## „Nutzung von Informations- und Kommunikationstechnologien“:

- Ein- und ausgehender dienstlicher E-Mail-Verkehr wird zur Wahrung gesetzlicher Aufbewahrungsfristen automatisch archiviert (10 Jahre)
- Internet-Verbindungsdaten (Datum, Uhrzeit, Website, IP-Adresse, ggf. Datenmengen) werden protokolliert und für 7 Tage gespeichert.
  - Kontrollen durch Systemadministratoren im Zusammenwirken mit dem betrieblichen Datenschutzbeauftragten und dem Betriebsrat sind möglich.
- Die private Nutzung der betrieblichen E-Mail-Adressen ist nicht gestattet.
- Private Nutzung von eigenen E-Mail-Adressen bei externem Provider und Internet ist nur kurzzeitig und gelegentlich gestattet.

1) <https://intranet.intern/personal/betriebsvereinbarungen>

# Passwörter

- Schützen Sie vertraulichen Informationen durch Passwörter.
- Verwenden Sie sichere Passwörter und vermeiden Sie Mehrfachverwendung.
- Geben Sie persönliche Passwörter oder Benutzerkennungen niemals weiter.
- Nutzen Sie zum Verwalten Ihrer persönlichen, dienstlichen Passwörter den Passwortmanager „KeePass“
  - auf neuer Hardware vorinstalliert
  - alternativ über Softwareantrag im Self-Service-Portal zu bestellen

# Löschen – Vernichten – Verlieren

- Entsorgen Sie dienstliche Dokumente ausschließlich in den dafür vorgesehenen Sammelbehältern oder schreddern Sie diese mit geeigneten Aktenvernichtern.
- Datenträger (USB-Sticks, Festplatten etc.) über KDI entsorgen.
- Leeren Sie nach dem Löschen von Dateien auch den Windows-Papierkorb.
- Melden Sie den unbeabsichtigten Verlust dienstlichen Daten **unverzüglich** Ihrem Vorgesetzten und / oder der betrieblichen DSB, z. B. wenn Sie Dokumente oder mobile Geräte oder Speicher wie USB-Sticks verlieren!
- Machen Sie sich mit den spezifischen Regelungen zu Datenschutz und IT-Sicherheit im Unternehmen und in ihrem Fachbereich vertraut!

# Verschlüsseln

- Nutzen Sie die gängigen Verschlüsselungsmöglichkeiten<sup>1)</sup> in der EWN:
  - Cryptshare (E-Mail)
  - VeraCrypt (längerfristige Verschlüsselung besonders sensibler Daten)
  - 7-Zip (einmalige Verschlüsselung von Dateien)
  - **Nicht geeignet** ist der Kennwortschutz von MS-Office.
- ! Die Anleitungen finden Sie im Intranet<sup>2)</sup>
- E-Mails und Telefaxe sind nicht sicherer als Postkarten! Versenden Sie vertrauliche Daten daher NICHT per Fax oder als unverschlüsselte E-Mail.
  - ! Kontrollieren Sie bei E-Mails die Empfängerliste, insbesondere bei der Nutzung der „Allen-Antworten-Funktion“.

1) Achtung: verschlüsselte Daten können NICHT wiederhergestellt werden, wenn das Passwort verloren geht oder die Datei beschädigt wird.

2) <https://intranet.intern/informationsshytechnik/anleitungen>

# Die Datenschutzbeauftragte

## Angela Bialke

- Meine Aufgabe ist insbesondere die Überwachung der Einhaltung des Datenschutzrechts.
- Dazu unterrichte und berate ich Sie hinsichtlich Ihrer Pflichten aber auch Ihrer Rechte nach den geltenden Datenschutzvorschriften und
- unterstütze Sie bei der Bewertung von technischen und organisatorischen Maßnahmen.
- Ich bin zur Geheimhaltung und Verschwiegenheit verpflichtet.
- Zu meinen Aufgaben gehört auch die Zusammenarbeit mit den Aufsichtsbehörden.

**Wir setzen Maßstäbe.  
Mit Sicherheit.**

**Vielen Dank!**

**Angela Bialke**

Telefon +49 38354 4 - 5307 | [datenschutz@ewn-gmbh.de](mailto:datenschutz@ewn-gmbh.de) | [www.ewn-gmbh.de](http://www.ewn-gmbh.de)