



SOFORT MELDEN

Datenpanne oder Verdacht? Unverzüglich melden!

Jeder Verstoß, Verlust oder Verdacht (verlorenes/gestohlenes Gerät, Fehlversand, unbefugter Zugriff, falsche KI-Eingabe ...) ist **sofort schriftlich** dem Datenschutzbeauftragten zu melden.

Vincent Wetterling · Tel. +49 (0) 5161 6030525 · info@datenfuersorge.de

Online: datenfuersorge.de/datenpanne

1 Schweigepflicht & Verschwiegenheit

- Absolutes Stillschweigen über alle bewohner-/kundenbezogenen sowie betrieblichen Angelegenheiten und Geschäftsgeheimnisse.
- Gilt **auch gegenüber Kolleg:innen**, die nicht mit der Aufgabe betraut sind.
- Die Schweigepflicht **endet nicht** mit dem Arbeitsverhältnis – sie gilt zeitlich unbegrenzt fort.
- Verstöße sind Dienstpflichtverletzungen, können **strafbar** sein und Schadensersatz auslösen.

2 Grundsätze (Art. 5 DSGVO)

Rechtmäßigkeit

Zweckbindung

Datenminimierung

Richtigkeit

Speicherbegrenzung

Vertraulichkeit

Leitsatz: „So viele Daten wie nötig, so wenige Daten wie möglich.“
Verbot mit Erlaubnisvorbehalt – Verarbeitung nur mit Rechtsgrundlage oder Einwilligung.

3 Unterlagen & Arbeitsplatz

- ✓ Schriftstücke wegschließen (Schrank, Dienstzimmer, Auto), Sichtschutz gegenüber Unbefugten.
- ✓ Bildschirm sperren und abmelden, wenn der Platz verlassen wird.
- ✗ Keine unautorisierte Mitnahme oder Kopie von Unterlagen.
- ✗ Daten nicht offen liegen lassen.

4 IT, Geräte & Übermittlung

- ✓ Nur passwortgeschützte Zugänge; Diensthandys gemäß Vorgaben nutzen.
- ✓ Versand nur über sichere Wege/Verbindungen.
- ✗ Keine Speicherung auf privaten/externen Medien (USB etc.).
- ✗ Keine unsicheren Wege wie Fax für sensible Daten.

5 Passwörter

- ✓ Für jeden Zugang ein **eigenes, starkes** Passwort (lang, Zeichenmix).
- ✓ Passwort-Manager nutzen.
- ✗ Passwörter niemals weitergeben oder notieren/sichtbar lassen.
- ✗ Keine simplen Muster (z. B. „Passwort123!“).

6 Auskünfte & Recht am eigenen Bild

- Bei Anfragen **Berechtigung der Person prüfen**, auf Mithörer achten.
- An Angehörige nur mit **schriftlicher Zustimmung** des Betroffenen.
- ✗ Keine Fotos/Videos/Audios von Arbeit/Bewohner:innen auf (privaten) Social-Media.
- Ausnahme: bei **lebenswichtigen Interessen** dürfen Daten weitergegeben werden.

7 Umgang mit KI (z. B. ChatGPT)

- ✗ Keine sensiblen/personenbezogenen Daten (Name, Diagnose, Medikamentenplan) in externe KI-Tools.
- ✓ Nur freigegebene Systeme; Einsatz **vorher mit dem DSB abstimmen**.
- ✓ KI-Ergebnisse sind Vorschläge – kritisch prüfen, Verantwortung bleibt beim Menschen.
- Versehenliche Eingabe? **Sofort melden** (Löschung extern meist nicht möglich).

8 Phishing erkennen

- Gefälschte Absender, Abfrage von Passwörtern/Daten, künstliche Dringlichkeit.
- Verdächtige Links (Ziel per Mouseover prüfen) und unerwartete Anhänge.
- Rechtschreibfehler, unpersönliche Anrede.
- ✗ Im Zweifel nicht klicken/öffnen – Absender über bekannten Weg verifizieren.

9 Rechte der Betroffenen – bei solchen Anliegen an den DSB verweisen

Auskunft (Art. 15)

Berichtigung (Art. 16)

Löschung (Art. 17)

Einschränkung (Art. 18)

Datenübertragbarkeit (Art. 20)

Widerspruch (Art. 21)

Beschwerde bei der Aufsichtsbehörde (Art. 77)

Ist eine Person nicht geschäftsfähig, sind Datenschutz-Anliegen mit dem rechtlichen Betreuer/Bevollmächtigten abzustimmen.