



Datenschutz im beruflichen Alltag

Inhaltsübersicht

1

Arbeiten im Büro

2

Mobiles Arbeiten

3

Entsorgung von
Papierdokumenten

4

Datenpannen

5

Anfertigung und
Veröffentlichung von Fotos



Arbeiten
im Büro

Datenschutzkonforme Gestaltung des Arbeitsplatzes (1)

- Unbefugte dürfen nicht auf personenbezogene Daten zugreifen und diese nicht einsehen können.
 - Insbesondere bei Kundenverkehr ist sicherzustellen, dass keine Möglichkeit der Einsichtnahme in personenbezogene Daten besteht.
 - Die Dokumente dürfen nicht offen auf dem Tisch liegen oder auf dem Bildschirm zu sehen sein.
- Verlässt der Mitarbeitende während der Arbeitszeit das Büro, ist der Bildschirmschoner mit Kennwortschutz zu aktivieren und alle Papierdokumente mit personenbezogenen Daten sind wegzuschließen („Clean desk“).
 - Ist dies nicht möglich, ist das Büro abzuschließen.
 - Dies gilt auch nach dem Ende der Arbeitszeit.

Datenschutzkonforme Gestaltung des Arbeitsplatzes (2)

- Sofern in der Einrichtung Kundenverkehr besteht, ist beim Führen von Telefonaten sicherzustellen, dass keine unbefugten Personen mithören können.
- Befindet sich der Drucker nicht im eigenen Büro und haben mehrere Personen darauf Zugriff, sind gedruckte Dokumente unverzüglich aus dem Drucker zu nehmen. Empfohlen wird „vertrauliches Drucken“ einzustellen.
- Nicht mehr benötigte Dokumente sind nach den geltenden dienstlichen Regeln zu vernichten.
- Elektronisch gespeicherte personenbezogene Daten sind unwiederbringlich zu löschen, sobald diese nicht mehr benötigt werden.
 - Zu beachten ist, dass die Daten bei einem „einfachen“ löschen in der Regel wiederhergestellt werden können.
 - Für eine unwiederbringliche Löschung von elektronisch gespeicherten personenbezogenen Daten sollte daher die IT hinzugezogen werden.
 - Das Löschkonzept ist zu beachten.

Anforderungen an die IT-Infrastruktur

- Mitarbeitenden ist ein individueller Account zur Verfügung zu stellen.
- Es ist sicherzustellen, dass die dienstlichen Endgeräte über essentielle Schutzmaßnahmen verfügen.
 - Es sollten aktuelle Anwendungs- und Systemsoftware, Schutz vor Schadsoftware und Firewall genutzt werden.
 - Updates sind regelmäßig und zeitnah durchzuführen.
 - Sperrung von USB-Zugängen und anderen Anschlüssen
 - An dienstliche Endgeräte sollte keine private Hardware (z. B. USB-Sticks, externe Festplatten) angeschlossen werden.
- Mobile elektronische Speicher (z. B. USB-Sticks, externe Festplatten) müssen verschlüsselt sein.
- Die dienstlichen Endgeräte müssen hinreichend vor dem Zugriff durch Unbefugte geschützt sein (z. B. Bitlocker, Nutzung starker Passwörter).

A person wearing glasses and a blue shirt is seen from the side, working on a laptop. The laptop screen displays a glowing shield icon with a padlock inside, set against a background of binary code. The scene is set in a blurred indoor environment, possibly a home office.

Mobiles Arbeiten

Datenschutzkonforme Gestaltung meines Arbeitsplatzes

- Die Anforderungen an das Mobile Arbeiten sind grundsätzlich mit den Anforderungen an die Arbeit im Büro vergleichbar.
- Eine Einsichtnahme und ein Zugriff durch Unbefugte ist zu verhindern.
 - Beim Verlassen des Arbeitsplatzes ist der Bildschirmschoner mit Kennwortschutz zu aktivieren.
 - Bei Laptops kann zusätzlich eine Sichtschutzfolie verwendet werden.
- Private und dienstliche Unterlagen sind voneinander zu trennen.
- Papierdokumente sind in abschließbaren Behältnissen aufzubewahren.



Transport dienstlicher Unterlagen und mobiler Endgeräte

- Dienstliche Unterlagen sind in verschlossenen Behältnissen zu transportieren.
- Mobile Endgeräte müssen mit einem sicheren Passwort bzw. einer sicheren PIN gesichert sein.
- Externe Speichermedien (z. B. externe Festplatten, USB-Sticks) müssen verschlüsselt sein.
- Dienstliche Unterlagen und mobile Endgeräte dürfen während des Transports zu keinem Zeitpunkt unbeaufsichtigt sein.

Dienstliches Telefonieren

- Sicherstellung, dass ein Mithören ausgeschlossen ist.
- Dritte dürfen nicht auf die im Telefonbuch des dienstlichen Smartphones gespeicherten beruflichen Kontakte zugreifen können.
- Werden private Smartphones genutzt, sind automatisch gespeicherte Anrufkontakte regelmäßig zu löschen und es sollte die Rufnummer unterdrückt werden.



Nutzung eines privaten oder offenen WLANs

- Computer muss zwingend über eine verschlüsselte Verbindung mit dem WLAN verbunden werden.
- Mitarbeitende müssen sich über eine sichere Verbindung in das Netz der verantwortlichen Stelle einwählen (VPN).
 - Achtung: Öffentliche Netzwerkzugänge (z. B. im Zug oder Hotel) dürfen nur genutzt werden, wenn Zugriff auf IT-Infrastruktur der verantwortlichen Stelle über eine sichere Verbindung erfolgt.



Drucken und Löschen im mobilen Arbeiten

- Dokumente sollten nur im Büro ausgedruckt, sofern kein dienstlicher Drucker zur Verfügung gestellt wird.
 - Ist ein Zugriff auf die Infrastruktur der verantwortlichen Stelle über eine sichere Verbindung eingerichtet, sollten dennoch keine Druckaufträge an die Drucker im Büro geschickt werden.
- Unterlagen sind zu sammeln und bei Gelegenheit im Büro nach den geltenden dienstlichen Regeln zu entsorgen.
- Sind Daten auf externen Datenträgern gespeichert, sind diese der verantwortlichen Stelle zu übergeben und von dieser unwiederbringlich zu löschen.

Ergänzende Hinweise zum mobilen Arbeiten

- Auch beim mobilen Arbeiten liegt die datenschutzrechtliche Verantwortung für eine datenschutzkonforme Verarbeitung der personenbezogenen Daten bei der verantwortlichen Stelle.
- Die verantwortliche Stelle hat daher das Recht und die Pflicht, in regelmäßigen Abständen die Einhaltung der datenschutzrechtlichen Vorschriften zu kontrollieren.
 - Die Durchführung ist vertraglich oder im Rahmen einer Dienstvereinbarung zu regeln.
- Für den Fall des Datenverlusts bzw. des Datenschutzverstoßes besteht eine Meldepflicht.
 - Die verantwortliche Stelle muss klare Meldewege regeln und jeden Mitarbeitenden darüber informieren, wem Datenverluste bzw. Datenschutzverstöße zu melden sind.

Anforderungen an die Aktenvernichtung (1)

- Papierakten, die personenbezogene Daten enthalten, dürfen nicht im normalen Hausmüll entsorgt werden. Üblicherweise werden Papierakten „geschreddert“.
 - Aktenvernichter gibt es in verschiedenen Sicherheitsausführungen.
- Bei der Entsorgung ist die sogenannte DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern“ zu beachten.
 - Dort werden drei Schutzklassen (normal, hoch und sehr hoch) und sieben Sicherheitsstufen definiert.
 - Welche Schutzklasse und welche Sicherheitsstufe anzuwenden ist, ist vom Schutzbedarf der personenbezogenen Daten abhängig.
 - Je vertraulicher die Daten sind, desto höher ist auch der Schutzbedarf.

Anforderungen an die Aktenvernichtung (2)

- Alternativ kann die Aktenvernichtung auch an einen externen Dienstleister ausgelagert werden.
 - Es ist sicherzustellen, dass der externe Dienstleister die geltenden Vorschriften und insbesondere die geltende DIN-Norm einhält (z.B. durch geeignetes Zertifikat).
- Der externe Dienstleister wird dann als Auftragsverarbeiter tätig.
 - Es ist ein Auftragsverarbeitungsvertrag nach § 30 DSGVO-EKD zu schließen.
 - Handelt es sich bei dem externen Dienstleister nicht um eine kirchliche Stelle, muss zusätzlich die Zusatzvereinbarung nach § 30 Abs. 5 DSGVO-EKD unterschrieben werden.
- Werden die Akten zur Vernichtung in die Entsorgungsfirma transportiert, ist sicherzustellen, dass die Akten vor dem Transport vor dem Zugriff durch Unbefugte geschützt aufbewahrt werden.
 - Dazu können z. B. speziell verschließbare Container verwendet werden.

A red triangular warning sign is positioned on the right side of a paved road. The sign is made of a reflective material and is supported by three black legs. In the background, there are green trees and a clear blue sky. A white circular overlay is placed on the left side of the image, containing the text 'Datenpannen' in a red serif font.

Datenpannen

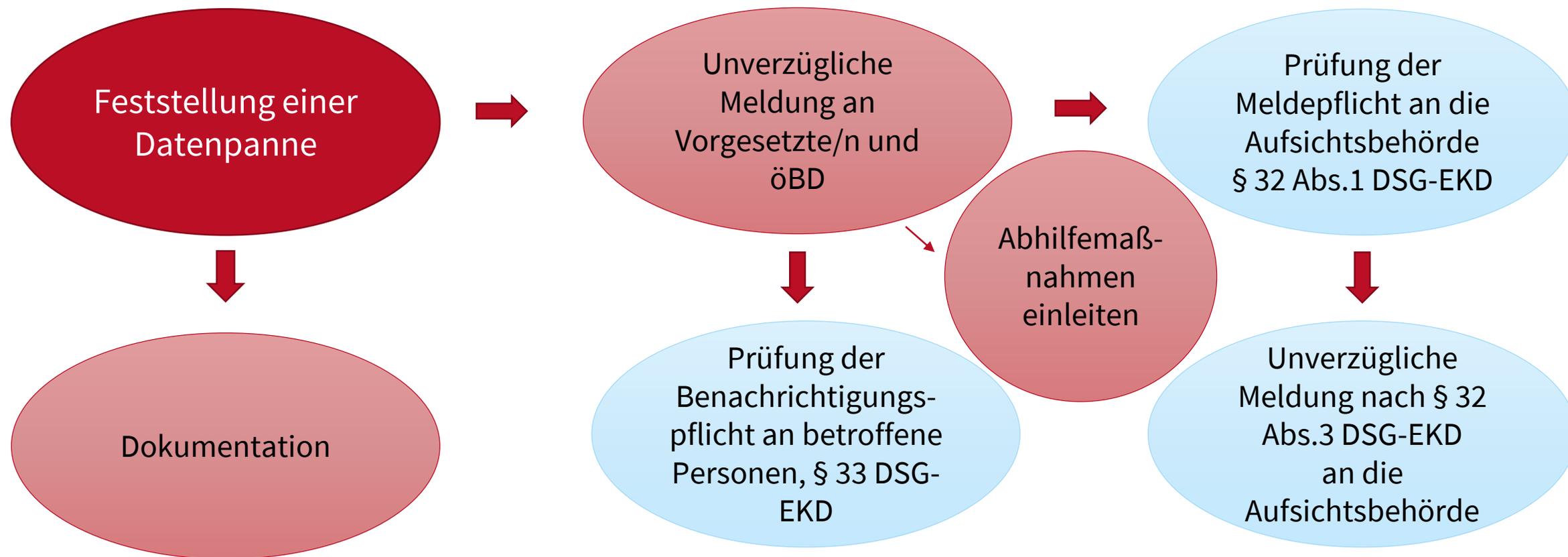
Was ist eine Datenpanne?

- Unter einer Datenpanne ist die Verletzung des Schutzes personenbezogener Daten zu verstehen.
 - Verletzung des Schutzes personenbezogener Daten ist in § 4 Nr. 14 DSGVO definiert.
- Darunter wird die Verletzung der Sicherheit verstanden, die
 - zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten oder
 - zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
- Die verantwortliche Stelle ist zur Meldung an die Aufsichtsbehörde verpflichtet, § 32 Abs. 1 S. 1 DSGVO.
- Ein Formular zur Meldung finden Sie unter: https://datenschutz.ekd.de/meldung_datenpannen/.

Datenpanne – Beispiele aus der Praxis und vorbeugende Maßnahmen

Häufige Datenpannen	Vorbeugende Maßnahmen
Diebstahl oder Verlust von Datenträgern (Fotokamera, Laptop, USB-Stick)	Sicheres Aufbewahren, Verschließen der Räume beim Verlassen, Regelmäßiges Löschen der Daten, Verschlüsselung
Unverschlüsselter Versand einer E-Mail mit personenbezogenen Daten	E-Mail mit personenbezogenen Daten immer verschlüsseln
Offenlegung / Übermittlung von personenbezogenen Daten an unberechtigte Dritte, Fehlversand, offener Mailverteiler	Prüfen, ob eine Offenlegung stattfinden darf: nur bei Vorliegen einer Rechtsgrundlage, prüfen ob E-Mail Adresse/ Postadresse korrekt sind, BCC anstatt CC
Phishing E-Mails werden geöffnet	Absender prüfen, Unbekannte / merkwürdige E-Mails nicht öffnen und der IT melden
Veröffentlichung von Kasualien, Fotos o. Ä. trotz eingelegtem Widerruf	Einwilligungs- und Widerrufsmanagement beachten

Umgang mit Datenpannen, §§ 32, 33 DSGVO-EKD



Wem ist die Datenpanne zu melden? (1)

- Die Meldung muss unverzüglich erfolgen, d.h. ohne schuldhaftes Zögern.
 - Es ist unerheblich, ob die Sicherheitslücke bereits geschlossen ist oder nicht.
- Die Datenpanne muss in der Meldung detailliert beschrieben werden, § 32 Abs. 3 DSGVO-EKD.
- Die Meldung ist nicht erforderlich, wenn die Verletzung voraussichtlich nur zu einem unerheblichen Risiko für die Rechte natürlicher Personen führt.
- Bei Vorliegen eines voraussichtlich hohen Risikos für die Rechte der betroffenen Person ist in der Regel eine Information an die betroffene Person erforderlich, § 33 Abs. 1 DSGVO-EKD.
 - Es sei denn, es liegt eine Ausnahme nach § 33 Abs. 3 DSGVO-EKD vor.

Wem ist die Datenpanne zu melden? (2)

- Verantwortliche Stelle muss im Einzelfall prüfen, ob die Verletzung zu einem nicht unerheblichen Risiko für die Rechte der betroffenen Person führt.
 - Bei der Prüfung ist die Eintrittswahrscheinlichkeit sowie die Schwere der Verletzung und der drohenden Rechtsverletzung zu berücksichtigen.
 - Es sind auch Art, Umfang und Umstände der zugrundeliegenden Verarbeitung zu beachten.
- Unterlässt die verantwortliche Stelle die Meldung an die Aufsichtsbehörde fahrlässig oder vorsätzlich, dann liegt eine Pflichtverletzung vor, die aufsichtliche Maßnahmen zur Folge haben kann.
 - Das gilt auch, wenn die betroffene Person bei Vorliegen der Voraussetzungen des § 33 Abs. 1 DSGVO nicht über die Verletzung des Schutzes personenbezogener Daten informiert wird.

An open camera with a film strip partially inserted into the back. In the foreground, there are two film strips and a film canister lying on a white surface. A semi-transparent circular overlay is positioned on the left side of the image, containing red text.

Anfertigung und
Veröffentlichung von
Fotos

Einleitende Hinweise

- Sollen bei einer Veranstaltung Fotos angefertigt werden, ist vorab zu prüfen, ob dies aus Sicht des Datenschutzes zulässig ist.
 - Hintergrund ist, dass bei der Anfertigung und Veröffentlichung von Fotos personenbezogene Daten verarbeitet werden.
- Entscheidend ist, ob auf den Fotos Personen zu sehen sind und ob die Personen auch identifiziert werden können.
 - Die Anforderungen an die Identifizierung sind gering.
 - Zur Identifizierung reicht es aus, wenn eine Person beispielsweise aufgrund ihrer Frisur oder Kleidung erkannt werden kann, auch wenn das Gesicht nicht zu sehen ist.
 - Es ist nicht erforderlich, dass die Person tatsächlich erkannt wird. Die Möglichkeit reicht aus.

Anfertigung von Fotos

- Für die Anfertigung von Fotos und der damit in Zusammenhang stehenden Verarbeitung von personenbezogenen Daten ist eine Rechtsgrundlage erforderlich.
- Bei der Anfertigung von Fotos ist das DSGVO-EKD zu beachten .
- Als Rechtsgrundlagen kommen § 6 Nr. 4 in Verbindung mit § 6 Nr. 8 DSGVO-EKD oder eine Einwilligung der betroffenen Person in Betracht.

Voraussetzungen nach § 6 Nr. 4 i.V.m. § 6 Nr. 8 DSGVO-EKD

- Die verantwortliche Stelle muss ein berechtigtes Interesse an der Anfertigung der Fotos haben.
- Es dürfen keine schutzwürdigen Interessen der betroffenen Person überwiegen.
 - Sofern die verantwortliche Stelle ein berechtigtes Interesse an der Anfertigung der Fotos hat, ist eine Interessenabwägung vorzunehmen.
 - Dabei ist beispielsweise zu berücksichtigen, in welchem Kontext die Fotos angefertigt werden und ob es sich bei den betroffenen Personen um besonders schutzwürdige Personen (z.B. Minderjährige) handelt.

Einwilligung, § 11 DSGVO-EKD

- Sind die Voraussetzungen von § 6 Nr. 4 i.V.m. § 6 Nr. 8 DSGVO-EKD nicht erfüllt, ist eine Einwilligung einzuholen.
- Die Anforderungen an eine wirksame Einwilligung sind in § 11 DSGVO-EKD geregelt:
 - Die Einwilligung muss in klarer und einfacher Sprache verfasst und hinreichend konkret sein.
 - Die betroffene Person muss umfänglich über die Bedeutung und die Folgen der Einwilligung informiert sein.
 - Die Einwilligung muss freiwillig erfolgen. Aus der Nichterteilung der Einwilligung dürfen sich keine negativen Folgen für die betroffene Person ergeben.
 - Es muss auf das jederzeit bestehende Widerrufsrecht hingewiesen werden.
- Aufgrund der Rechenschaftspflicht aus § 5 Abs. 2 DSGVO-EKD sollte die Einwilligung stets schriftlich eingeholt werden.

Veröffentlichung von Fotos

- Sollen die angefertigten Fotos anschließend veröffentlicht werden, liegt eine weitere Verarbeitung von personenbezogenen Daten vor, für die eine weitere Rechtsgrundlage erforderlich ist.
- Bei der Veröffentlichung von Fotos ist das Kunsturhebergesetz (KunstUrhG) zu beachten.
- Nach § 22 KunstUrhG ist bei der Veröffentlichung von Bildnissen grundsätzlich eine Einwilligung der betroffenen Person einzuholen. Ausnahmen von der Einwilligungspflicht sind in § 23 KunstUrhG geregelt.
- Bei der Einholung der Einwilligung ist darauf hinzuweisen, wo die Fotos veröffentlicht werden sollen. Auch diese Einwilligung sollte stets schriftlich eingeholt werden.
- Sollen die Fotos im Internet veröffentlicht werden, ist zusätzlich auf das Risiko hinzuweisen, dass einmal im Internet veröffentlichte Fotos nicht oder nur unter erheblichem Aufwand wieder gelöscht werden können.