Schulung für Mitarbeitende



Einführung in den Datenschutz

Grundlagen und Anwendung – mit Beispielen aus der Praxis

Gerd Kopp · Datenschutzbeauftragter · @gerds-it.de

Ablauf

45 Minuten in vier Teilen

4 Min.	Einstieg: Worum es beim Datenschutz eigentlich geht
14 Min.	Grundlagen: Welche Daten, welche Regeln, wer ist wer
18 Min.	Praxis: Sieben Fälle aus dem Arbeitsalltag – und was bei einer Datenpanne zu tun ist
9 Min.	Folgen, Quiz, zehn Regeln zum Mitnehmen und Ihre Fragen

Worum es geht

Hinter jedem Datensatz steht ein Mensch.

Frage in die Runde: Was wäre Ihnen unangenehm, wenn es plötzlich Ihr Nachbar über Sie wüsste?

Grundlagen

DSGVO und BDSG – was gilt?

DSGVO – EU-Verordnung

Gilt seit Mai 2018 direkt in der ganzen EU und hat Vorrang.

- Grundsätze und Rechtsgrundlagen
- Rechte der Betroffenen
- Pflichten, Datenpannen, Bußgelder

BDSG – deutsches Gesetz

Ergänzt die DSGVO nur dort, wo sie Spielraum lässt.

- Pflicht zum Datenschutzbeauftragten (§ 38)
- Beschäftigtendaten (§ 26)
- Bußgeld und Strafe (§§ 41–43)

Weitere Gesetze

Für Einzelthemen gelten Spezialregeln, z. B.:

- KUG: Fotos von Personen
- TDDDG: Cookies auf der Website
- AO, HGB: Aufbewahrungsfristen

Lesehilfe: „Art.“ steht für die DSGVO, „§“ für ein deutsches Gesetz. Im Konflikt gilt die DSGVO.

Grundlagen

Was sind personenbezogene Daten?

Alles, was sich einem bestimmten Menschen zuordnen lässt. (Art. 4 Nr. 1 DSGVO)

Alltägliche Daten

- Name, Anschrift, Geburtsdatum
- E-Mail, auch m.maier@firma.de
- Foto, Stimme, Kfz-Kennzeichen
- Kundennummer, IP-Adresse
- Bankverbindung, Gehalt

Besonders geschützt (Art. 9 DSGVO)

- Gesundheit, z. B. eine Diagnose
- Religion – etwa über die Kirchensteuer
- Gewerkschaftszugehörigkeit
- Herkunft, Biometrie, politische Meinung
- Sexualleben, sexuelle Orientierung

Faustregel: Lässt sich mit vertretbarem Aufwand herausfinden, wer gemeint ist, gilt der Datenschutz. (Erwägungsgrund 26 DSGVO)

Grundlagen

Verarbeiten heißt: jeder Umgang mit Daten

Die DSGVO gilt für Daten im Computer und für geordnete Papierablagen – Ordner, Karteikarten, Akten. (Art. 2 Abs. 1, Art. 4 Nr. 6 DSGVO)

Erfassen | **Speichern** | **Ansehen** | **Weitergeben** | **Ändern** | **Löschen**

> **Beispiel:** Sie schlagen in der Kundenkartei eine Telefonnummer nach. Schon das ist eine Verarbeitung – auf Papier genauso wie am Bildschirm. (Art. 4 Nr. 2 DSGVO)

Grundlagen

Die Grundregeln der DSGVO (Art. 5)

Regel	Was das im Alltag heißt
Rechtmäßig und offen (Abs. 1 lit. a)	Nur mit gutem Grund – und Betroffene wissen Bescheid.
Zweckbindung (Abs. 1 lit. b)	Rechnungsadressen landen nicht ungefragt im Newsletter.
Datenminimierung (Abs. 1 lit. c)	Für ein Angebot braucht es kein Geburtsdatum.
Richtigkeit (Abs. 1 lit. d)	Umzug gemeldet? Adresse sofort ändern.
Speicherbegrenzung (Abs. 1 lit. e)	Bewerbungen nach Absage nach ca. 6 Monaten löschen.
Sicherheit (Abs. 1 lit. f)	Abschließen, starke Passwörter, Bildschirm sperren.
Rechenschaft (Abs. 2)	Wir müssen nachweisen können, dass wir uns daran halten.

Grundlagen

Ohne Grund keine Verarbeitung

Jede Verarbeitung braucht eine Rechtsgrundlage (Art. 6 DSGVO) – meist eine dieser vier:

Vertrag

Kundenadresse für Lieferung und Rechnung.

Art. 6 Abs. 1 lit. b

Gesetz

Rechnungen aufbewahren, Lohndaten an Finanzamt und Sozialversicherung melden.

Art. 6 Abs. 1 lit. c; § 147 AO, § 257 HGB

Berechtigtes Interesse

Kamera im Lager gegen Diebstahl – mit Hinweisschild und nur so viel wie nötig.

Art. 6 Abs. 1 lit. f; Art. 13

Einwilligung

Foto der Mitarbeiterin auf der Website: freiwillig und jederzeit widerrufbar.

Art. 6 Abs. 1 lit. a; Art. 7

Gut zu wissen: Eine Einwilligung ist jederzeit widerrufbar. (Art. 7 Abs. 3 DSGVO)

Grundlagen

Die Rechte der Betroffenen

Auskunft	Was ist über mich gespeichert? (Art. 15)
Berichtigung	Falsche Daten korrigieren (Art. 16)
Löschung	Daten entfernen, wenn kein Grund mehr besteht (Art. 17)
Einschränkung	Daten sperren statt löschen (Art. 18)
Übertragung	Daten in gängigem Format herausgeben (Art. 20)
Widerspruch	Zum Beispiel gegen Werbung (Art. 21)

Antwortfrist

1 Monat

ab Eingang der Anfrage – auch wenn gerade Urlaub ist.

Art. 12 Abs. 3 DSGVO

Anfrage bekommen? Sofort an Geschäftsleitung und Datenschutzbeauftragten weitergeben.

Grundlagen

Wer ist wer?

Das Unternehmen	Ist „Verantwortlicher“: entscheidet, wofür Daten genutzt werden – und haftet. (Art. 4 Nr. 7, Art. 24 DSGVO)
Sie als Mitarbeitende	Arbeiten im Auftrag des Unternehmens und sind zur Vertraulichkeit verpflichtet. (Art. 29, Art. 32 Abs. 4 DSGVO)
Dienstleister	Lohnbüro, IT-Firma, Cloud-Anbieter: brauchen einen Vertrag zur Auftragsverarbeitung (AVV). (Art. 28 DSGVO)
Datenschutzbeauftragter (DSB)	Berät und kontrolliert – und ist Ihr Ansprechpartner, auf Wunsch vertraulich. (Art. 37–39 DSGVO, § 38 BDSG)
Aufsichtsbehörde	In Baden-Württemberg der Landesbeauftragte (LfDI): prüft Beschwerden, ordnet an, verhängt Bußgelder. (Art. 57, 58, 83 DSGVO)

Teil 2 · Praxis

Sieben Fälle aus dem Arbeitsalltag

Alle so oder ähnlich schon passiert. Bei jedem Fall fragen wir: Was ist schiefgelaufen – und wie geht es richtig?

Praxis · Fall 1 von 7

Der offene Verteiler

Die Situation

Die Einladung zum Kundenabend geht an 80 Kunden. Alle Adressen stehen sichtbar im An- oder CC-Feld.

Das Problem

Jeder Empfänger sieht die E-Mail-Adressen aller anderen. Das ist eine Datenpanne – Aufsichtsbehörden haben dafür schon Bußgelder verhängt.

Art. 4 Nr. 12, Art. 5 Abs. 1 lit. f, Art. 32, Art. 33 DSGVO

So geht's richtig

- Mehrere externe Empfänger: immer BCC
- Bei vielen Empfängern ein Newsletter-Werkzeug nutzen
- Vor dem Senden prüfen, was die Autovervollständigung eingesetzt hat
- Passiert? Sofort melden

Praxis · Fall 2 von 7

Schnell mal per WhatsApp

Die Situation

Der Monteur fotografiert den Schaden beim Kunden und schickt Bild, Name und Adresse über sein privates WhatsApp an den Chef.

Das Problem

WhatsApp überträgt das Adressbuch an den Anbieter – samt Telefonnummern von Kunden, die nie gefragt wurden. Und Firmendaten liegen auf dem Privathandy.

Art. 6 Abs. 1, Art. 32 DSGVO

So geht’s richtig

- Nur die vom Betrieb freigegebenen Apps nutzen
- Kundendaten nicht auf private Geräte
- Im Zweifel kurz fragen

Praxis · Fall 3 von 7

Fotos für Website und Social Media

Die Situation

Für die Website werden Fotos vom Team und vom fertigen Auftrag gemacht. Auf einem sieht man den Kunden, auf einem anderen sein Kennzeichen.

Das Problem

Ohne Einwilligung keine Veröffentlichung. Und wer das Unternehmen verlässt, kann verlangen, dass sein Foto verschwindet.

Art. 6 Abs. 1 lit. a, Art. 7 Abs. 3, Art. 17 DSGVO; § 22 KUG

So geht’s richtig

- Vorher schriftlich einwilligen lassen
- Gesichter, Kennzeichen und Hausnummern unkenntlich machen
- Ehemalige zeitnah von Website und Kanälen nehmen

Praxis · Fall 4 von 7

Die Auskunftsanfrage

Die Situation

Ein ehemaliger Mitarbeiter, im Streit gegangen, verlangt per E-Mail Auskunft über alle gespeicherten Daten. Die Mail liegt zwei Wochen im Sammelpostfach.

Das Problem

Die Frist ist ein Monat. Zu späte oder lückenhafte Auskunft kann Schadenersatz kosten – Arbeitsgerichte haben dafür schon Beträge zugesprochen.

Art. 12 Abs. 3, Art. 15, Art. 82 DSGVO

So geht's richtig

- Sofort an Geschäftsleitung und Datenschutzbeauftragten
- Eingangsdatum festhalten
- Identität prüfen
- Vollständig antworten: Personalakte, E-Mails, Zeiterfassung

Praxis · Fall 5 von 7

Kurz die KI fragen

Die Situation

Eine Kollegin kopiert eine Kundenbeschwerde mit Name, Adresse und Vertragsdetails in einen kostenlosen KI-Chat, um eine freundliche Antwort zu formulieren.

Das Problem

Die Daten gehen an einen Anbieter, oft außerhalb der EU, ohne Vertrag mit uns. Kostenlose Versionen nutzen Eingaben häufig zum Training.

Art. 5 Abs. 1 lit. b, Art. 28, Art. 44 ff. DSGVO

So geht’s richtig

- Nur vom Betrieb freigegebene Werkzeuge nutzen
- Namen und Details vorher entfernen („Kunde X“)
- Im Zweifel fragen

Praxis · Fall 6 von 7

Am Arbeitsplatz

Die Situation

Mittagspause: Der Bildschirm ist offen, Lieferscheine liegen am Empfang. Ein Anrufer: „Hier ist die Krankenkasse, ich brauche kurz die Adresse von Herrn Maier."

Das Problem

Wer vorbeikommt, liest mit. Und am Telefon weiß niemand, wer wirklich dran ist – eine beliebte Masche.

Art. 5 Abs. 1 lit. f, Art. 6 Abs. 1, Art. 32 DSGVO

So geht's richtig

- Beim Aufstehen sperren: Windows-Taste + L
- Empfang und Schreibtisch frei von Unterlagen
- Keine Auskünfte am Telefon – Rückruf über bekannte Nummer
- Papier in den Aktenvernichter, nicht ins Altpapier

Praxis · Fall 7 von 7

Der falsche Klick

Die Situation

Eine E-Mail vom „Paketdienst“: Bitte Lieferung bestätigen. Ein Klick, Passwort eingegeben – am nächsten Morgen sind die Dateien verschlüsselt.

Das Problem

Kundendaten sind womöglich abgeflossen. Das Unternehmen muss das innerhalb von 72 Stunden der Aufsichtsbehörde melden.

Art. 33 Abs. 1, Art. 34 DSGVO

So geht’s richtig

- Sofort melden – Fehler passieren, Verschweigen ist das eigentliche Problem
- Nichts löschen, Gerät vom Netz nehmen
- Passwort umgehend ändern lassen

Praxis

Datenpanne – was jetzt?

Schritt 1

Bemerken

Verdächtige Mail, verlorenes Handy, falscher Empfänger

Art. 4 Nr. 12

→

Schritt 2 · Ihre Aufgabe

Sofort melden

an die Geschäftsleitung – auch am Wochenende

Art. 29, Art. 32 Abs. 4

→

Schritt 3

Bewerten

Geschäftsleitung und DSB prüfen das Risiko

Art. 33 Abs. 5, Art. 39

→

Schritt 4

Melden

an die Behörde binnen 72 Stunden, bei hohem Risiko auch an Betroffene

Art. 33 Abs. 1, Art. 34

72 Stunden ab Kenntnis, auch am Wochenende. EU-Lockerungen geplant, nicht beschlossen.

Folgen

Was passieren kann

Bußgeld

20 Mio. €

oder 4 % des weltweiten Jahresumsatzes – der Höchstrahmen. Kleine Betriebe zahlen weniger, aber spürbar.

Art. 83 Abs. 5 DSGVO

Schadenersatz

Art. 82

Betroffene können Ersatz verlangen – auch für immaterielle Schäden wie Ärger und Kontrollverlust.

Art. 82 Abs. 1 DSGVO

Haftung Einzelner

Persönlich

Wer Daten für private Zwecke abruft, kann selbst ein Bußgeld bekommen – das ist schon mehrfach passiert.

Art. 83 DSGVO; § 42 BDSG

> Dazu kommt der Schaden, der in keinem Bescheid steht: Kunden, die das Vertrauen verlieren.

Folgen

Fälle aus der Aufsichtspraxis

Deutsche Wohnen	Archivsystem konnte alte Mieterdaten nicht löschen. Bußgeld 2019: 14,5 Mio. €, später vom Landgericht Berlin auf 900.000 € gesenkt. (Art. 5 Abs. 1, Art. 25 DSGVO)
Niedersachsen 2025	Bußgelder u. a. gegen Firmen, deren Fahrzeugkameras den öffentlichen Verkehr filmten, und gegen Privatleute mit Dashcams. (Art. 6 Abs. 1 DSGVO)
Einzelne Beschäftigte	Bußgelder gegen Mitarbeitende, die Daten unbefugt abfragten – etwa bei Polizei und Zulassungsstelle. (Art. 4 Nr. 7, Art. 83 DSGVO)

> **Gemeinsamer Nenner:** Kein Hackerangriff, sondern Alltag – fehlendes Löschen, Kameras, Neugier.

Quiz

Richtig oder falsch?

„m.maier@firma.de ist kein personenbezogenes Datum – ist ja dienstlich.“	**Falsch: gehört zu einer Person (Art. 4 Nr. 1).**
„Eine Auskunftsanfrage muss innerhalb eines Monats beantwortet sein.“	**Richtig: ab Eingang (Art. 12 Abs. 3).**
„Wenn mir ein Fehler passiert, behebe ich ihn am besten still selbst.“	**Falsch: sofort melden, 72 Stunden (Art. 33).**
„Bewerbungsunterlagen dürfen nach einer Absage nicht ewig liegen bleiben.“	**Richtig: nach ca. 6 Monaten löschen (Art. 5 Abs. 1 lit. e).**
„Der Anrufer kennt die Kundennummer, also darf ich Auskunft geben.“	**Falsch: Rückruf über bekannte Nummer (Art. 6, Art. 32).**

Zum Mitnehmen

Zehn Regeln für den Alltag

1. Nur die Daten erfassen, die wirklich gebraucht werden. (Art. 5 Abs. 1 lit. c)
2. Bildschirm sperren, sobald Sie aufstehen. (Art. 32)
3. Mails an mehrere externe Empfänger: BCC. (Art. 5 Abs. 1 lit. f)
4. Kundendaten nur in Firmen-Apps, nie auf dem Privathandy. (Art. 32)
5. Keine Kundendaten in frei verfügbare KI-Chats. (Art. 28, Art. 44 ff.)
6. Fotos nur mit Einwilligung veröffentlichen. (Art. 6 Abs. 1 lit. a, Art. 7)
7. Am Telefon keine Auskünfte an Unbekannte. (Art. 6 Abs. 1)
8. Papier mit Daten in den Aktenvernichter. (Art. 32)
9. Anfragen von Betroffenen sofort weitergeben. (Art. 12 Abs. 3)
10. Fehler sofort melden – lieber einmal zu viel. (Art. 33)

Zum Nachschlagen

Wichtige Links

Aufsichtsbehörde	Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) baden-wuerttemberg.datenschutz.de
Datenpanne melden	Online-Formular des LfDI für Meldungen nach Art. 33 DSGVO baden-wuerttemberg.datenschutz.de/datenpanne-melden
DSGVO im Volltext	Amtliche deutsche Fassung im Amtsblatt der EU (EUR-Lex) eur-lex.europa.eu/eli/reg/2016/679/oj/deu
BDSG im Volltext	Bundesdatenschutzgesetz beim Bundesjustizministerium gesetze-im-internet.de/bdsg_2018
Praxishilfen	Kurzpapiere der Datenschutzkonferenz zu vielen Einzelthemen datenschutzkonferenz-online.de/kurzpapiere.html

Ihre Fragen

Fragen? Jederzeit.

Datenschutzbeauftragter	Gerd Kopp
Vertraulich	Ihre Fragen und Hinweise werden vertraulich behandelt.
Bei Datenpannen	Sofort an Geschäftsleitung und Datenschutzbeauftragten – auch außerhalb der Bürozeiten.