GANZ EINFACH

Datenschutz ohne Panik

DSGVO für Vereine, Praxen und kleine Betriebe



Danilo Sieren

G A N Z E I N F A C H

Band 67

Datenschutz ohne Panik

DSGVO für Vereine, Praxen und kleine Betriebe

Danilo Sieren

GANZ EINFACH

Die Reihe GANZ EINFACH erklärt Technik und Alltagsthemen so, wie es eine gute Freundin oder ein guter Freund am Küchentisch tun würde: geduldig, ehrlich und mit vielen Beispielen. Jeder Band steht für sich, und wo ein anderer Band ein Thema vertieft, steht ein Hinweis im Text.

Impressum und Hinweise zur Entstehung stehen auf der letzten Seite dieses Buches.

Vorwort

Kaum ein Gesetz hat in Deutschland so viel Verunsicherung ausgelöst wie die Datenschutz-Grundverordnung. Als sie im Mai 2018 wirksam wurde, löschten Vereine ihre Mitgliederfotos von der Webseite, Bäckereien hängten seitenlange Aushänge neben die Kasse, und manche Arztpraxis ließ Patienten im Wartezimmer nur noch mit Nummern aufrufen. Ehrenamtliche Kassierer fürchteten Bußgelder in Millionenhöhe, Handwerksbetriebe kauften teure Musterpakete, und in Elterngruppen kursierten Gerüchte, man dürfe keine Klassenfotos mehr machen.

Acht Jahre später hat sich die Aufregung gelegt, die Verunsicherung nicht. Viele kleine Organisationen wissen bis heute nicht genau, was sie eigentlich tun müssen. Sie haben irgendwann eine Datenschutzerklärung aus einem Generator kopiert, unterschreiben Einwilligungen, die sie selbst nicht verstehen, und hoffen, dass niemand nachfragt. Andere haben so viel Angst vor Fehlern, dass sie sinnvolle Dinge unterlassen: Sie schicken keine Rundmails mehr, veröffentlichen keine Ergebnisse, nehmen keine Fotos mehr auf. Beides ist schade.

Dieses Buch will die Panik nehmen, ohne den Datenschutz kleinzureden. Denn hinter dem sperrigen Gesetz steckt ein vernünftiger Gedanke: Menschen sollen wissen und mitbestimmen können, was mit Informationen über sie geschieht. Wer Mitgliederlisten führt, Patientenakten verwaltet oder Kundendaten speichert, trägt Verantwortung für Menschen, die ihm vertrauen. Diese Verantwortung lässt sich mit gesundem Menschenverstand, ein paar festen Gewohnheiten und einigen Vorlagen gut tragen.

Gerade jetzt ist vieles in Bewegung. Die Europäische Kommission hat im November 2025 vorgeschlagen, die DSGVO mit dem sogenannten Digital-Omnibus an einigen Stellen zu vereinfachen. Bund und Länder haben angekündigt, die deutsche Sonderregel abzuschaffen, nach der schon Betriebe mit zwanzig Beschäftigten einen Datenschutzbeauftragten brauchen. Beides war bei Redaktionsschluss im November 2026 noch nicht beschlossen. Das Buch erklärt, was heute gilt, was sich ändern könnte und warum die meisten Pflichten auch nach einer Reform bestehen bleiben.

Es beginnt mit den Grundlagen: den wichtigsten Begriffen, den Grundsätzen, den Rechtsgrundlagen und der Einwilligung. Es zeigt, welche Unterlagen man braucht, wie man Daten schützt, Dienstleis-

ter einbindet und mit Auskunftsanfragen und Datenpannen umgeht. Dann folgen drei Teile für die drei Welten, für die dieses Buch geschrieben ist: den Verein, die Praxis und den kleinen Betrieb. Zum Schluss geht es um Webseiten, Messenger, Cloud, künstliche Intelligenz, Videoüberwachung, Bußgelder und darum, wie man Datenschutz dauerhaft organisiert, ohne dass er zur Last wird.

Durch das Buch begleitet dich Sabine Kröger. Sie ist 52 Jahre alt, Praxismanagerin in einer Physiotherapiepraxis in Herne und ehrenamtliche Schriftführerin in einem Turnverein mit gut vierhundert Mitgliedern. Ihr Mann Frank führt einen Elektrobetrieb mit sieben Beschäftigten. In derselben Woche im Frühjahr landen bei allen dreien Datenschutzprobleme auf dem Tisch: ein Kinderfoto in einer Messengergruppe, ein Befund im falschen Briefumschlag und das Schreiben eines Anwalts, der für einen ehemaligen Mitarbeiter Auskunft verlangt.

Du brauchst für dieses Buch keine juristischen Vorkenntnisse. Paragrafen und Artikel nenne ich dort, wo sie dir helfen, etwas nachzuschlagen. Die Kästen mit der Überschrift Vertiefung kannst du beim ersten Lesen überspringen.

Danilo Sieren, Dortmund, im November 2026

So arbeitest du mit diesem Buch

Das Buch ist in fünf Teile gegliedert.

Die Kapitel 1 bis 7 legen die Grundlagen: warum Datenschutz keine Panik braucht, welche Begriffe man kennen muss, nach welchen Grundsätzen und auf welcher Rechtsgrundlage Daten verarbeitet werden dürfen, wie eine Einwilligung richtig eingeholt wird, was für besonders sensible Daten gilt und wie man Menschen informiert. Die Kapitel 8 bis 14 behandeln die Pflichten jeder Organisation: das Verzeichnis der Verarbeitungstätigkeiten, technische und organisatorische Maßnahmen, Auftragsverarbeitung, den Datenschutzbeauftragten, die Rechte der Betroffenen, Löschen und Aufbewahren sowie den Umgang mit Datenpannen. Die Kapitel 15 bis 17 sind dem Verein gewidmet, die Kapitel 18 bis 20 der Praxis, die Kapitel 21 und 22 dem kleinen Betrieb. Die Kapitel 23 bis 28 behandeln Themen, die alle betreffen: Webseiten und Cookies, Messenger und Cloud, künstliche Intelligenz, Videoüberwachung, Aufsicht und Bußgelder sowie die Organisation des Datenschutzes im Jahreslauf.

Wer schnell wissen will, was er mindestens tun muss, liest Kapitel 1, Kapitel 8 und die passende Checkliste im Anhang. Wer eine Auskunftsanfrage beantworten muss, schlägt Kapitel 12 auf. Wer gerade eine Datenpanne entdeckt hat, beginnt sofort mit Kapitel 14, denn dort läuft eine Frist.

Die Bausteine jedes Kapitels

Jedes Kapitel beginnt mit einer Erklärung in normaler Sprache. Tabellen fassen Pflichten, Fristen und Unterschiede zusammen. Kästen mit der Überschrift **Vertiefung** erklären Hintergründe. **Achtung**-Kästen warnen vor typischen Fehlern. **Tipp**-Kästen enthalten Kniffe aus der Praxis. In den **Lernprojekt**-Kästen begleitest du Sabine und Frank Kröger, das Team der Praxis und den Vorstand des Turnvereins.

In der **Werkstatt** setzt du das Gelernte Schritt für Schritt um. Am Ende jedes Kapitels beantworte ich **Häufige Fragen** und fasse in **Kurz gesagt** das Wichtigste zusammen. Im Anhang findest du ein Glossar, Checklisten für Verein, Praxis und Betrieb, Muster für ein Verarbeitungsverzeichnis, eine Einwilligung, eine Antwort auf eine Auskunftsanfrage und ein Protokoll für Datenpannen, eine Über-

sicht über Aufbewahrungsfristen, Fragen zum Selbsttest und die Adressen der Aufsichtsbehörden.

Rechtsstand

Das Buch gibt den Rechtsstand vom November 2026 wieder. Grundlage sind die Datenschutz-Grundverordnung, das Bundesdatenschutzgesetz, das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, das Kunsturhebergesetz und die einschlägigen Berufs- und Sozialgesetze. Wo Änderungen geplant, aber noch nicht beschlossen sind, sage ich das ausdrücklich.

> **ACHTUNG** **Kein Ersatz für Rechtsberatung**
>
> Dieses Buch erklärt die Regeln so, dass du sie im Alltag anwenden kannst. Es kann aber nicht jeden Einzelfall abdecken. Wenn es um viel geht, etwa bei einer Anfrage der Aufsichtsbehörde, einer Abmahnung, einer Klage oder einer größeren Datenpanne, solltest du dir fachkundigen Rat holen. Viele Landessportbünde, Kammern, Innungen und Berufsverbände bieten ihren Mitgliedern kostenlose Erstberatung an.

Inhalt

Vorwort....3
So arbeitest du mit diesem Buch....5
Warum Datenschutz keine Panik braucht....9
Die wichtigsten Begriffe....17
Die Grundsätze der DSGVO....25
Rechtsgrundlagen: Wann darf ich Daten verarbeiten?....32
Einwilligung richtig einholen....40
Besondere Kategorien: Gesundheit, Religion und mehr....47
Informieren: Datenschutzhinweise, die man lesen kann....55
Das Verzeichnis von Verarbeitungstätigkeiten....62
Technische und organisatorische Maßnahmen....69
Dienstleister und Auftragsverarbeitung....77
Braucht ihr einen Datenschutzbeauftragten?....84
Die Rechte der Betroffenen....91
Löschen und Aufbewahren....98
Datenpannen erkennen und melden....106
Der Verein: Mitglieder, Satzung und Ehrenamt....114
Fotos und Videos....122
Webseite, Newsletter und soziale Netzwerke im Verein....129
Die Praxis: Schweigepflicht und Patientendaten....136
Praxisalltag: Empfang, Telefon und Kommunikation....143
Praxissoftware, Patientenakte und Online-Angebote....150
Der Betrieb: Kunden, Angebote und Werbung....157
Beschäftigtendaten....164
Webseite, Cookies und Tracking....171
Messenger, Cloud und Videokonferenz....178
Künstliche Intelligenz und Datenschutz....185
Videoüberwachung....191
Aufsicht, Bußgelder, Abmahnungen und Schadensersatz....197
Datenschutz organisieren: der Jahresplan....204
Glossar....210
Checkliste Verein....213
Checkliste Praxis....214
Checkliste Betrieb....215
Muster: Eintrag im Verzeichnis....216
Muster: Einwilligung in Fotos....218
Muster: Antwort auf eine Auskunftsanfrage....220
Muster: Protokoll einer Datenpanne....222

Aufbewahrungsfristen 224
Fragen zum Selbsttest.....226
Aufsichtsbehörden und Anlaufstellen.....228
Nachwort.....230
Quellen und weiterführende Links 231
Ausführliches Inhaltsverzeichnis 233
Stichwortverzeichnis.....245
Impressum 249

KAPITEL 1

Warum Datenschutz keine Panik braucht

Datenschutz hat einen schlechten Ruf. Er gilt als bürokratisch, weltfremd und gefährlich: ein Gestrüpp aus Paragrafen, in dem man sich nur verfangen kann. Dieses Bild ist verständlich, aber es ist falsch. Datenschutz ist im Kern eine Frage des Anstands im Umgang mit Informationen über andere Menschen. Dieses Kapitel zeigt, worum es eigentlich geht, warum kleine Organisationen keine Angst haben müssen und wo der Ernst trotzdem beginnt.

Worum es eigentlich geht

Stell dir vor, du gibst deinem Sportverein deine Anschrift, dein Geburtsdatum und deine Kontonummer. Du erwartest, dass der Verein damit deine Mitgliedschaft verwaltet und den Beitrag abbucht. Du erwartest nicht, dass deine Daten an eine Versicherung verkauft werden, dass die Mitgliederliste offen auf einem Tisch im Vereinsheim liegt oder dass ein Foto von deinem Kind ohne Rückfrage im Internet landet. Genau diese Erwartungen schützt der Datenschutz.

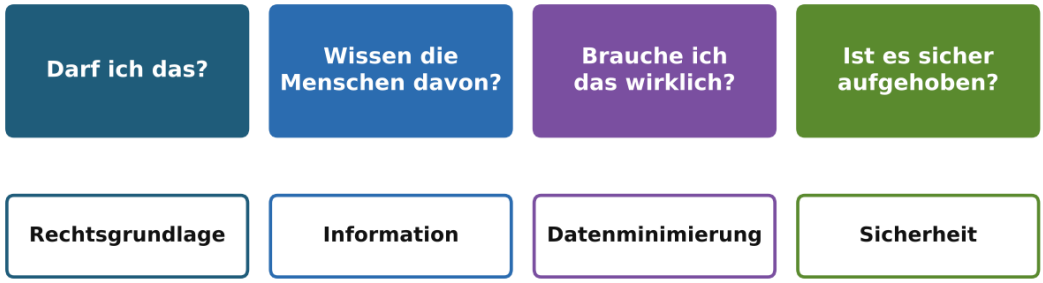
Die Datenschutz-Grundverordnung, kurz **DSGVO**, formuliert das in juristischer Sprache. Sie schützt nicht Daten, sondern Menschen. Ihr Ziel ist, dass jeder selbst bestimmen kann, wer was über ihn weiß und was damit geschieht. Das Bundesverfassungsgericht hat dafür schon 1983 im Volkszählungsurteil den Begriff **informationelle Selbstbestimmung** geprägt. Die DSGVO ist die europäische Fassung dieses Gedankens.

Daraus folgen vier einfache Fragen, die man sich bei jedem Umgang mit Daten stellen kann:

Frage	was dahintersteht
Darf ich das überhaupt?	Jede Verarbeitung braucht eine Rechtsgrundlage.
Wissen die Menschen davon?	Betroffene müssen informiert werden.
Brauche ich das wirklich?	Nur so viele Daten wie nötig, so lange wie nötig.

Frage	was dahintersteht
Ist es sicher aufgehoben?	Daten müssen vor Verlust und fremdem Zugriff geschützt werden.

Wer diese vier Fragen ehrlich beantwortet, hat den größten Teil des Datenschutzes schon verstanden. Der Rest sind Werkzeuge, mit denen man die Antworten festhält und nachweist.



Die vier Grundfragen des Datenschutzes: Darf ich das? Wissen die Menschen davon? Brauche ich das wirklich? Ist es sicher aufgehoben?

Für wen die DSGVO gilt

Die DSGVO gilt für fast jeden, der personenbezogene Daten verarbeitet, egal wie klein er ist. Es gibt keine Ausnahme für Vereine, für Ehrenamtliche oder für Kleinbetriebe. Der Kegelclub mit zwölf Mitgliedern ist ebenso betroffen wie der Großkonzern. Die einzige wichtige Ausnahme betrifft rein persönliche und familiäre Tätigkeiten: Wer privat ein Adressbuch führt, Urlaubsfotos von Freunden macht oder Geburtstage im Kalender notiert, fällt nicht unter die DSGVO. Diese sogenannte **Haushaltsausnahme** endet aber dort, wo jemand für einen Verein, eine Praxis oder einen Betrieb tätig wird.

Wer	gilt die DSGVO?
Privatperson mit Adressbuch	nein, Haushaltsausnahme
Eltern, die Fotos im Familienchat teilen	in der Regel nein
eingetragener oder nicht eingetragener Verein	ja

Wer	gilt die DSGVO?
Ehrenamtliche, die für den Verein Listen führen	ja, der Verein ist verantwortlich
Arztpraxis, Physiotherapie, Heilpraktiker	ja, mit strengeren Regeln für Gesundheitsdaten
Handwerksbetrieb, Laden, Selbstständige	ja
Kirchengemeinde	eigenes kirchliches Datenschutzrecht, inhaltlich ähnlich

Viele kleine Organisationen glauben, die DSGVO sei für Konzerne gemacht und gelte für sie nur am Rande. Richtig ist: Die Grundpflichten gelten für alle. Einige Pflichten, etwa die Bestellung eines Datenschutzbeauftragten oder die Datenschutz-Folgenabschätzung, hängen von Größe und Risiko ab. Und die Aufsichtsbehörden berücksichtigen bei ihrer Arbeit sehr wohl, ob sie es mit einem ehrenamtlich geführten Verein oder mit einem internationalen Unternehmen zu tun haben.

Was die Panik ausgelöst hat

Die Angst vor der DSGVO hatte mehrere Ursachen. Die Bußgelder von bis zu zwanzig Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes klangen bedrohlich. Abmahnanwälte kündigten an, Verstöße massenhaft zu verfolgen. Beratungsfirmen verkauften Pakete mit Hunderten Seiten Dokumentation. Und vieles war tatsächlich unklar, weil es noch keine Urteile und keine eingespielte Praxis gab.

Seitdem hat sich viel geklärt. Die befürchtete Abmahnwelle gegen kleine Vereine ist ausgeblieben. Die Aufsichtsbehörden setzen bei kleinen Organisationen in aller Regel zuerst auf Beratung und Hinweise. Bußgelder treffen vor allem Unternehmen, die Daten systematisch missbrauchen, Sicherheitsmängel über lange Zeit ignorieren oder Anfragen der Behörde nicht beantworten. Wer sich erkennbar bemüht, seine Pflichten zu erfüllen, und auf Hinweise reagiert, hat wenig zu befürchten.

> **VERTIEFUNG** **Woher die hohen Summen kommen**
>
> Die DSGVO kennt zwei Bußgeldrahmen: bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes für Verstöße gegen organisatorische Pflichten, bis zu zwanzig Millionen Euro oder vier Prozent für Ver-

> stöße gegen Grundsätze und Betroffenenrechte. Diese Obergrenzen sollen verhindern, dass große Konzerne Bußgelder aus der Portokasse zahlen. Für die Bemessung im Einzelfall sind Art, Schwere und Dauer des Verstoßes, Vorsatz oder Fahrlässigkeit, die Zusammenarbeit mit der Behörde und die wirtschaftliche Leistungsfähigkeit maßgeblich. Ein Turnverein wird nicht nach denselben Maßstäben behandelt wie eine internationale Plattform.

Wo der Ernst beginnt

Keine Panik heißt nicht kein Ernst. Datenschutzverstöße können Menschen wirklich schaden. Ein Befund im falschen Umschlag kann eine Krankheit offenlegen, die jemand vor seinem Arbeitgeber verbergen wollte. Eine offen verschickte E-Mail mit hundert Adressen im Empfängerfeld verrät, wer Mitglied in einer Selbsthilfegruppe ist. Ein gestohlener Laptop mit ungesicherter Kundenliste kann zu Betrug und Identitätsdiebstahl führen. Ein Kinderfoto in einer öffentlichen Gruppe kann in falsche Hände geraten.

Hinzu kommen rechtliche Folgen, die auch kleine Organisationen treffen können:

Folge	Beispiel
Anordnung der Aufsichtsbehörde	Löschung von Daten, Änderung von Abläufen
Bußgeld	bei schweren oder hartnäckigen Verstößen
Schadensersatz	Betroffene verlangen Geld für materiellen oder immateriellen Schaden
Unterlassungsanspruch	Betroffene verlangen, dass eine Verarbeitung aufhört
Strafrecht	bei Verletzung der Schweigepflicht oder unbefugter Weitergabe
Vertrauensverlust	Mitglieder treten aus, Patienten und Kunden wechseln

Der letzte Punkt ist oft der wichtigste. Ein Verein, eine Praxis oder ein Handwerksbetrieb lebt vom Vertrauen der Menschen. Wer mit ihren Daten sorgfältig umgeht, zeigt Respekt. Wer nachlässig ist, verspielt mehr als ein Bußgeld.

Datenschutz und Datensicherheit

Zwei Begriffe werden oft verwechselt. **Datenschutz** fragt, ob und wie personenbezogene Daten verwendet werden dürfen. **Datensi-**

cherheit, auch Informationssicherheit, fragt, wie Daten vor Verlust, Manipulation und unbefugtem Zugriff geschützt werden. Datensicherheit betrifft alle Daten, auch Konstruktionspläne oder Rezepturen. Datenschutz betrifft nur Daten über Menschen.

Beide hängen eng zusammen. Die DSGVO verlangt ausdrücklich, dass personenbezogene Daten sicher verarbeitet werden. Ein Verein, der seine Mitgliederliste ohne Passwort auf einem USB-Stick herumträgt, verstößt gegen den Datenschutz, weil er die Sicherheit vernachlässigt. Umgekehrt nützt die beste Verschlüsselung nichts, wenn Daten erhoben werden, die man gar nicht hätte erheben dürfen.

> **TIPP Der Blick von außen**
>
> Eine gute Übung für jede Organisation: Stell dir vor, du wärst das Mitglied, der Patient oder der Kunde. Würdest du wollen, dass mit deinen Daten so umgegangen wird? Würdest du dich wundern, wenn du erfährst, wer alles deine Telefonnummer kennt? Was dich als Betroffenen stören würde, ist meist auch rechtlich ein Problem.

Ein realistisches Ziel

Kein Verein, keine Praxis und kein Betrieb ist datenschutzrechtlich perfekt. Selbst große Unternehmen mit eigenen Rechtsabteilungen machen Fehler. Das Ziel ist nicht Perfektion, sondern ein solides Fundament: Man weiß, welche Daten man hat, warum man sie hat, wer sie sieht und wie lange man sie aufbewahrt. Man hat die wichtigsten Unterlagen beisammen. Man weiß, was zu tun ist, wenn jemand Auskunft verlangt oder etwas schiefgeht. Und man überprüft das alles einmal im Jahr.

Stufe	Merkmal
Grundlage	Überblick über die Daten, Verzeichnis, Datenschutzhinweise
Sicherheit	Passwörter, Updates, Sicherungen, Zugriffsrechte
Verträge	Auftragsverarbeitung mit Dienstleistern
Abläufe	Auskunft, Löschung, Datenpanne geregelt
Pflege	jährliche Überprüfung, Schulung, Anpassung

Wer diese fünf Stufen erreicht, ist besser aufgestellt als die meisten kleinen Organisationen in Deutschland. Dieses Buch führt Schritt für Schritt dorthin.

LERNPROJEKT Drei Briefe in einer Woche

Es ist ein Montag im März, als Sabine Kröger in der Physiotherapiepraxis Lindner in Herne die Post öffnet. Ein Patient schickt einen Brief zurück, den er von der Praxis bekommen hat: Darin liegt nicht sein eigener Therapiebericht, sondern der einer Patientin mit demselben Nachnamen. Am Mittwochabend klingelt Sabines Telefon. Jana Albers, die Jugendwartin des Turnvereins, in dem Sabine Schriftführerin ist, klingt aufgelöst. Eine Mutter, Ilona Berger, habe in der Elterngruppe geschrieben, sie werde sich bei der Datenschutzbehörde beschweren, weil Jana Fotos vom Kinderturnen in die Gruppe gestellt hat, auf denen auch ihre Tochter zu sehen ist. Am Freitag legt Sabines Mann Frank beim Abendessen einen Brief auf den Tisch. Ein Anwalt verlangt im Namen von Dennis Wolter, einem ehemaligen Gesellen von Frank, Auskunft über alle Daten, die der Elektrobetrieb über ihn gespeichert hat, binnen eines Monats. Frank fragt, ob er das einfach ignorieren kann. Sabine sagt, sie wisse es nicht. Am Samstag ruft sie Carsten Vogt an, einen Schulfreund, der seit Jahren als externer Datenschutzbeauftragter für mehrere Firmen arbeitet. Carsten hört sich alles an und sagt: »Drei verschiedene Probleme, ein gemeinsamer Kern. Keine Panik. Aber auch nicht liegen lassen.«

Eine kurze Geschichte des Datenschutzes

Datenschutz ist keine Erfindung der Europäischen Union. Das erste Datenschutzgesetz der Welt trat 1970 in Hessen in Kraft, als Behörden begannen, Daten mit Großrechnern zu verarbeiten. 1977 folgte das erste Bundesdatenschutzgesetz. Das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 machte aus dem Datenschutz ein Grundrecht: Jeder Mensch soll grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten bestimmen.

Jahr	Ereignis
1970	Hessisches Datenschutzgesetz, das erste der Welt
1977	erstes Bundesdatenschutzgesetz
1983	Volkszählungsurteil, Recht auf informationelle Selbstbestimmung
1995	europäische Datenschutzrichtlinie
2009	Datenschutz wird Grundrecht in der Charta der Grundrechte der EU

Jahr	Ereignis
2016	Datenschutz-Grundverordnung verabschiedet
2018	DSGVO gilt in allen Mitgliedstaaten
2025	Vorschlag des Digital-Omnibus zur Änderung der DSGVO

Die DSGVO hat das Rad also nicht neu erfunden. Vieles, was 2018 als neu empfunden wurde, galt in Deutschland schon vorher. Neu waren vor allem die einheitliche Geltung in ganz Europa, die höheren Bußgelder und die Rechenschaftspflicht. Wer vor 2018 ordentlich gearbeitet hatte, musste wenig ändern. Wer den Datenschutz vorher ignoriert hatte, bekam plötzlich viel zu tun, und daher stammt ein Teil der Panik.

Datenschutz in Kirchengemeinden und kirchlichen Einrichtungen

Kirchen haben in Deutschland das Recht, ihren Datenschutz selbst zu regeln, wenn ihre Regeln mit der DSGVO im Einklang stehen. Die katholische Kirche wendet das Gesetz über den Kirchlichen Datenschutz an, die evangelische Kirche das Datenschutzgesetz der EKD. Beide sind inhaltlich eng an die DSGVO angelehnt, haben aber eigene Aufsichtsbehörden und teilweise eigene Begriffe.

Für Kirchengemeinden, kirchliche Kitas, Diakonie- und Caritas-Einrichtungen gelten also im Wesentlichen dieselben Grundsätze wie in diesem Buch, mit anderen Paragrafen. Vereine, die einer Kirche nahestehen, aber rechtlich selbstständig sind, fallen dagegen oft unter die DSGVO. Im Zweifel hilft die Datenschutzstelle des jeweiligen Bistums oder der Landeskirche.

Werkstatt: Eine erste Bestandsaufnahme

1. Schreibe auf, für welche Organisation du Verantwortung trägst oder mitarbeitest: Verein, Praxis, Betrieb.
2. Notiere, welche Gruppen von Menschen dort vorkommen: Mitglieder, Patienten, Kunden, Beschäftigte, Interessenten, Lieferanten.
3. Schreibe zu jeder Gruppe auf, welche Daten ungefähr gespeichert werden.
4. Notiere, wo diese Daten liegen: Papierordner, Computer, Programm, Cloud, Telefon.

5. Beantworte für jede Gruppe die vier Grundfragen aus diesem Kapitel mit Ja, Nein oder Weiß nicht.
6. Markiere alle Antworten mit Nein oder Weiß nicht. Das ist deine erste Aufgabenliste.

Häufige Fragen

Gilt die DSGVO auch für einen kleinen Verein ohne Geld? Ja. Die Größe und die finanzielle Lage spielen für die Frage, ob die DSGVO gilt, keine Rolle. Sie spielen aber eine Rolle dabei, welche Maßnahmen angemessen sind und wie eine Behörde reagiert.

Haften Ehrenamtliche persönlich? In der Regel haftet der Verein als Verantwortlicher. Ehrenamtliche Vorstandsmitglieder und Helfer sind durch die Haftungsbeschränkungen im Vereinsrecht weitgehend geschützt, solange sie nicht vorsätzlich oder grob fahrlässig handeln.

Muss ich jetzt alles auf einmal umsetzen? Nein. Beginne mit dem Überblick über deine Daten und mit den wichtigsten Unterlagen. Viele weitere Punkte lassen sich nach und nach erledigen.

Ist Datenschutz nicht einfach Bürokratie? Ein Teil der Pflichten besteht aus Dokumentation, das stimmt. Diese Dokumentation hilft aber auch, den Überblick zu behalten, und schützt im Streitfall.

Was ist der Unterschied zwischen der DSGVO und dem BDSG? Die DSGVO ist eine europäische Verordnung, die unmittelbar gilt. Das BDSG ergänzt sie in Bereichen, in denen die DSGVO den Mitgliedstaaten Spielraum lässt, etwa beim Datenschutzbeauftragten oder bei Gesundheitsdaten.

Gilt die DSGVO auch für die Schweiz? Nein. Die Schweiz hat ein eigenes Datenschutzgesetz. Für Daten, die aus der EU in die Schweiz gehen, gilt ein Angemessenheitsbeschluss.

> KURZ GESAGT **Das Wichtigste aus Kapitel 1**
>
> Die DSGVO schützt Menschen, nicht Daten. Sie gilt für Vereine, Praxen und Betriebe jeder Größe, nicht aber für rein private Tätigkeiten. Vier Grundfragen tragen weit: Darf ich das? Wissen die Menschen davon? Brauche ich das wirklich? Ist es sicher aufgehoben? Die Aufsichtsbehörden setzen bei kleinen Organisationen zuerst auf Beratung. Keine Panik heißt aber nicht kein Ernst: Verstöße können Menschen schaden und Vertrauen zerstören.

KAPITEL 2

Die wichtigsten Begriffe

Wer die DSGVO verstehen will, muss einige Begriffe kennen. Sie klingen sperrig, sind aber mit Beispielen schnell zu durchschauen. Die meisten Missverständnisse im Datenschutz entstehen dadurch, dass Begriffe zu eng oder zu weit verstanden werden. Dieses Kapitel erklärt die wichtigsten Begriffe aus Artikel 4 der DSGVO und zeigt, wie sie im Alltag eines Vereins, einer Praxis und eines Betriebs aussehen.

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Das klingt abstrakt, ist aber sehr weit. Dazu gehören nicht nur Name, Anschrift und Geburtsdatum, sondern auch eine Telefonnummer, eine E-Mail-Adresse, ein Kfz-Kennzeichen, ein Foto, eine Stimme auf einer Aufnahme, eine IP-Adresse, eine Kundennummer, eine Krankheit, ein Kontostand oder die Notiz »kommt immer zu spät«.

Bestimmbar heißt: Die Person muss nicht namentlich genannt sein. Es genügt, dass man sie mit vertretbarem Aufwand herausfinden kann. »Die Kassiererin des Turnvereins« ist eine bestimmbare Person, wenn es nur eine Kassiererin gibt. »Der Patient mit dem Termin dienstags um acht« ist bestimmbar, wenn man den Kalender hat.

Beispiel	personenbezogen?
Name und Anschrift eines Mitglieds	ja
Foto vom Sommerfest mit erkennbaren Gesichtern	ja
Teilnehmerzahl eines Kurses	nein, wenn keine Person erkennbar ist
Kundennummer ohne Namen	ja, wenn sie einer Person zugeordnet werden kann
Statistik »40 Prozent der Mitglieder sind über 60«	nein
E-Mail-Adresse info@firma.de	in der Regel nein
E-Mail-Adresse sabine.kroeger@firma.de	ja

Beispiel	personenbezogen?
Daten einer GmbH	nein, nur Menschen sind geschützt
Daten eines Einzelunternehmers	ja, weil sie eine Person betreffen
Daten Verstorbener	nein nach DSGVO, aber Schweigepflicht gilt weiter

Nicht geschützt sind also Daten über Unternehmen als solche, anonyme Statistiken und Daten Verstorbener. Für Verstorbene gelten aber andere Regeln weiter, etwa die ärztliche Schweigepflicht.

Besondere Kategorien

Einige Daten sind besonders sensibel, weil ihr Missbrauch Menschen besonders schaden kann. Die DSGVO nennt sie **besondere Kategorien personenbezogener Daten**:

- Herkunft und ethnische Zugehörigkeit,
- politische Meinungen,
- religiöse und weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- genetische und biometrische Daten zur Identifizierung,
- Gesundheitsdaten,
- Daten zum Sexualleben und zur sexuellen Orientierung.

Für diese Daten gelten strengere Regeln, die Kapitel 6 erklärt. Für Praxen sind sie der Normalfall. Aber auch Vereine und Betriebe haben öfter damit zu tun, als sie denken: Ein Sportverein, der Unverträglichkeiten für das Zeltlager abfragt, verarbeitet Gesundheitsdaten. Ein Betrieb, der Krankmeldungen ablegt oder die Konfession für die Kirchensteuer kennt, ebenso.

Verarbeitung

Verarbeitung ist jeder Umgang mit personenbezogenen Daten, ob mit oder ohne Computer. Das Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln, Veröffentlichen, Abgleichen, Einschränken, Löschen und Vernichten: alles ist Verarbeitung. Selbst das bloße Ansehen einer Mitgliederliste gehört dazu.

Für Papier gilt die DSGVO, wenn die Daten in einem **Dateisystem** gespeichert sind oder werden sollen, also nach bestimmten Merkmalen geordnet. Ein alphabetisch sortierter Karteikasten mit Mit-

gliedskarten fällt darunter, ein Stapel loser Notizzettel in der Schublade eher nicht. In der Praxis spielt diese Unterscheidung selten eine Rolle, weil fast alle Organisationen ihre Daten heute irgendwie geordnet ablegen.

Verantwortlicher

Verantwortlicher ist, wer über Zwecke und Mittel der Verarbeitung entscheidet. Das ist in der Regel die Organisation selbst, nicht der einzelne Mitarbeiter:

Situation	Verantwortlicher
Turnverein führt Mitgliederliste	der Verein, vertreten durch den Vorstand
Praxis führt Patientenakten	die Praxisinhaberin oder der Praxisinhaber
Elektrobetrieb speichert Kundendaten	die GmbH, vertreten durch den Geschäftsführer
Mitarbeiterin am Empfang gibt Termine ein	die Praxis, nicht die Mitarbeiterin
Kassierer führt Liste auf privatem Laptop	der Verein, für den er tätig ist

Der Verantwortliche muss alle Pflichten der DSGVO erfüllen und das auch nachweisen können. Er kann Aufgaben an andere übertragen, die Verantwortung bleibt aber bei ihm.

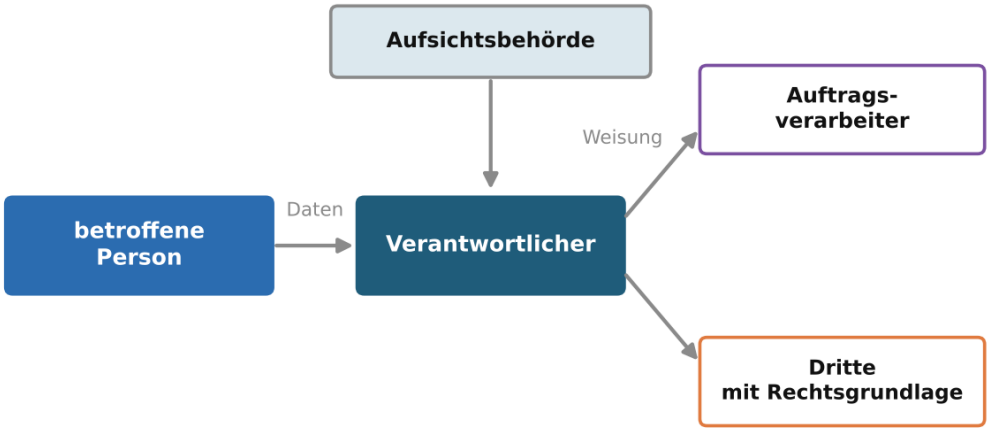
Manchmal entscheiden zwei Organisationen gemeinsam über eine Verarbeitung. Dann spricht die DSGVO von **gemeinsam Verantwortlichen**. Ein Beispiel ist ein Verein, der gemeinsam mit seinem Landesverband ein Online-Portal für Wettkampfmeldungen nutzt, dessen Funktionen beide festlegen. Gemeinsam Verantwortliche müssen in einer Vereinbarung regeln, wer welche Pflichten übernimmt.

Auftragsverarbeiter

Auftragsverarbeiter ist, wer personenbezogene Daten im Auftrag und nach Weisung eines Verantwortlichen verarbeitet. Typische Beispiele sind der Anbieter der Praxissoftware, der die Daten in seinem Rechenzentrum speichert, der Newsletter-Dienst, der die E-Mails eines Vereins verschickt, oder der IT-Dienstleister, der die Rechner eines Betriebs wartet.

Der Auftragsverarbeiter darf die Daten nicht für eigene Zwecke nutzen. Er handelt wie ein verlängerter Arm des Verantwortlichen. Dafür braucht es einen Vertrag nach Artikel 28 DSGVO, den Kapitel 10 erklärt.

Nicht jeder Dienstleister ist Auftragsverarbeiter. Ein Steuerberater, eine Bank, ein Rechtsanwalt oder die Post handeln eigenverantwortlich. Sie erhalten Daten, verarbeiten sie aber nach eigenen beruflichen Regeln. Mit ihnen schließt man keinen Auftragsverarbeitungsvertrag.



Die Rollen im Datenschutz: Die betroffene Person vertraut ihre Daten dem Verantwortlichen an, der Auftragsverarbeiter arbeitet in seinem Auftrag, Dritte erhalten Daten nur mit Rechtsgrundlage, die Aufsichtsbehörde wacht über alles.

Betroffene Person und Dritte

Betroffene Person ist der Mensch, um dessen Daten es geht: das Mitglied, der Patient, die Kundin, der Beschäftigte, der Bewerber. Die DSGVO gibt ihr eine Reihe von Rechten, die Kapitel 12 vorstellt.

Dritter ist jeder, der weder betroffene Person noch Verantwortlicher noch Auftragsverarbeiter ist und auch nicht unter der Aufsicht eines dieser Beteiligten arbeitet. Gibt ein Verein Mitgliederdaten an einen Sponsor weiter, ist der Sponsor Dritter. Dafür braucht der Verein eine eigene Rechtsgrundlage.

Empfänger ist jeder, dem Daten offengelegt werden, also auch ein Auftragsverarbeiter oder eine Behörde. In den Datenschutzhinweisen muss man angeben, an welche Empfänger Daten gehen.