DATENSCHUTZAKTUELL FEB 2026

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

Themenheft:
**Erfolgreich Daten schützen in Ihrer Vereinsarbeit**


# SCHRITT FÜR SCHRITT: SO WIRD IHR VEREIN DATENSCHUTZ-KONFORM

## *Vom Vorsatz zur Umsetzung*

*Liebe Leserin, lieber Leser,*

*„Wir sind doch nur ein kleiner Verein – da gilt das doch nicht für uns!" Diesen Satz höre ich oft, wenn es um Datenschutz geht. Doch genau hier liegt ein Irrtum: Die Datenschutz-Grundverordnung gilt für fast alle Vereine – unabhängig von Größe, Zweck oder Ehrenamtlichkeit.*

*Wichtig ist deshalb, den eigenen Verein datenschutzsicher aufzustellen: jetzt starten und Strukturen schaffen, die zum Vereinsalltag passen. Mit dieser Ausgabe zeigen wir Ihnen, wie Datenschutz im Verein gelingt – Schritt für Schritt und mit System.*

*Viele Grüße*

*Dr. Anna-Kathrin Mauch,*
*Rechtsanwältin und Redakteurin*

**Ihre Expertin für Datenschutz**
Dr. Anna-Kathrin Mauch ist Rechtsanwältin und Europajuristin mit Erfahrung im Vertrags- und Datenschutzrecht. Sie bringt Datenschutz verständlich und praxisnah auf den Punkt.

# Inhalt



**Zum neuen Onlinebereich!**
**www.privacyxperts.de/login**

**Expertensprechstunde:**
**https://t1p.de/andreas-wuertz**


## Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Autorin:
Dr. Anna-Kathrin Mauch, Rottweil

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | Marco2811; Seite 1: Adobe Stock | vegefox.com

Erscheinungsweise: 26-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Wo Menschen in einem Verein zusammenkommen, werden Daten verarbeitet.

# DSGVO – für welche Vereine sie gilt und für welche nicht

**Vielleicht haben auch Sie sich bereits gefragt, ob die Datenschutz-Grundverordnung (DSGVO) in Ihrem Verein überhaupt zu beachten ist. Die kurze, klare Antwort lautet: ja, sehr wahrscheinlich schon. Denn auch kleine oder ehrenamtlich geführte Vereine fallen häufig unter die DSGVO. Lassen Sie uns gemeinsam prüfen, ob das auch auf Ihren Verein zutrifft, damit Sie Klarheit haben und Risiken vermeiden – und datenschutzrechtlich auf der sicheren Seite sind.**

## Wann die DSGVO im Verein greift

Die DSGVO gilt immer dann, wenn personenbezogene Daten verarbeitet werden – also sobald personenbezogene Daten beispielsweise erhoben, gespeichert, geordnet, übermittelt, verändert oder gelöscht werden. Zu den personenbezogenen Daten gehören bereits grundlegende Informationen wie Name, Kontaktdaten oder Bankverbindungen. Und genau das passiert im Vereinsalltag in der Regel schon ganz am Anfang: Bereits im Aufnahmeantrag werden meistens Name, Anschrift, Geburtsdatum, Telefonnummer, E-Mail-Adresse oder Bankverbindung abgefragt.

Auch darüber hinaus gibt es zahlreiche typische Verarbeitungssituationen:

- Mitgliederverwaltung – Einzug von Beiträgen, Versand von Einladungen und Informationen
- Teilnehmer- und Anwesenheitslisten – z. B. für Trainings, Proben, Kurse oder Sitzungen
- Fotos und Videos bei Vereinsveranstaltungen – Veröffentlichung auf Website, Social Media oder in Chroniken
- Kommunikation über WhatsApp, Messenger oder E-Mail-Verteiler – zur Organisation von Terminen und Abläufen
- Verwaltung von Spenden – Erfassung von Namen, Adressen und ggf. Bankdaten für Spendenquittungen

Trifft auch nur **eines** dieser Beispiele auf Ihren Verein zu, gilt die DSGVO vollständig – mit allen daraus folgenden Pflichten. Die gute Nachricht: Mit einem klaren Überblick und passenden Maßnahmen ist Datenschutz im Verein meist gut handhabbar.

### Datenschutz ist Vorstandsaufgabe

**Für den Datenschutz ist grundsätzlich der Vereinsvorstand verantwortlich – nicht „irgendjemand" oder nur die IT. Nach der DSGVO gilt der Verein als sogenannter Verantwortlicher (Art. 4 Nr. 7 DSGVO). Damit trifft die Pflicht zur Umsetzung und Kontrolle letztlich den Vorstand, der den Verein nach außen vertritt (§ 26 Abs. 1 Satz 2 Bürgerliches Gesetzbuch). Der Vorstand muss deshalb jederzeit nachweisen können, dass die Datenschutzregeln eingehalten werden.**

## Wann die DSGVO hingegen nicht gilt

Die DSGVO findet ausnahmsweise keine Anwendung, wenn personenbezogene Daten ausschließlich privat oder im familiären Kreis verarbeitet werden. Entscheidend ist dabei nicht, ob sich eine Gruppe „Verein" nennt oder welchem Zweck sie dient, sondern ob die konkrete Datenverarbeitung rein privat bleibt.

Beispiel: Drei Freunde treffen sich regelmäßig zum privaten Schachspielen und nennen sich „Schachclub Samstagabend". Es existieren keine Mitgliederliste, keine Webseite, keine Werbung, kein Beitragseinzug und es werden keine personenbezogenen Daten strukturiert erhoben oder gespeichert. Hier handelt es sich rechtlich nicht um einen Verein im datenschutzrechtlichen Sinne, sondern um eine rein private Freizeitgruppe. Die DSGVO gilt in diesem Fall nicht (vgl. Art. 2 Abs. 2 Buchst. c DSGVO).

## Mythos versus Realität im Vereinsdatenschutz

Was viele im Vereinsalltag glauben, stimmt datenschutzrechtlich so nicht. Die folgenden Gegenüberstellungen helfen, typische Fehlannahmen einzuordnen und rechtlich korrekt zu bewerten. Sie zeigen praxisnah, wo vermeintliche Selbstverständlichkeiten im Vereinsalltag mit den Vorgaben der DSGVO kollidieren. Viele dieser Annahmen begegnen uns regelmäßig in der Praxis. Vielleicht finden auch Sie in der folgenden Übersicht einen Irrtum wieder, dem Sie bislang unterlegen sind.

| Mythos | Realität |
|---|---|
| „Unser Verein ist klein, das betrifft uns nicht." | Die DSGVO gilt unabhängig von der Vereinsgröße. Sobald personenbezogene Daten verarbeitet werden – und das tut in der Regel jeder Verein –, greifen die gesetzlichen Anforderungen. |
| „Wir sind kein eingetragener Verein – also nicht betroffen." | Die Rechtsform spielt keine Rolle. Entscheidend ist allein, ob ein Verein personenbezogene Daten verarbeitet – nicht, ob er im Vereinsregister steht. In der Praxis sehr häufig: kleine Sportgruppen, Förderkreise, Chöre etc. |
| „Wir verdienen kein Geld, deshalb greift Datenschutz nicht." | Gewinnerzielungsabsicht ist irrelevant. Auch gemeinnützige und rein ehrenamtliche Organisationen müssen dieselben Vorgaben einhalten wie wirtschaftliche Akteure. |
| „Wir speichern nur Telefonnummern, keine sensiblen Daten." | Auch Telefonnummern sind personenbezogene Daten. Bereits die Möglichkeit, eine Person identifizieren zu können, genügt für die Anwendbarkeit der DSGVO. |
| „Eine Excel-Liste auf dem privaten Laptop ist keine Datenverarbeitung." | Doch – auch das Speichern ist eine Verarbeitung. Achtung: Auf privaten Geräten kann dies unzulässig sein, wenn kein ausreichender Schutz besteht. |
| „Wir veröffentlichen nur harmlose Gruppenfotos – das ist okay." | Fotos gelten als personenbezogene Daten und erfordern eine Rechtsgrundlage. Ohne Einwilligung oder eine andere Erlaubnisnorm dürfen Bilder nicht veröffentlicht oder weitergegeben werden. Ausnahmen nach § 23 KunstUrhG sind möglich (z. B. Fotos von Veranstaltungen), ersetzen aber nicht jede Einwilligung. |
| „Im Ehrenamt wird nichts passieren – wir machen es ja für einen guten Zweck." | Guter Zweck schützt nicht vor DSGVO-Pflichten und möglichen Bußgeldern. Aufsichtsbehörden haben ausdrücklich bestätigt, dass Verstöße auch bei Vereinen geahndet werden können. |

## Was passiert, wenn Ihr Verein die DSGVO nicht beachtet?

Datenschutz wirkt im Vereinsalltag oft abstrakt – bis etwas schiefläuft. Datenschutz im Verein sollten Sie nicht auf die leichte Schulter nehmen: Wird er vernachlässigt, können schnell verschiedene Risiken entstehen. Werden die Vorgaben der DSGVO nicht eingehalten, bleiben die Folgen selten rein theoretisch. Vielmehr zeigen sich die Konsequenzen oft unmittelbar – rechtlich, finanziell und organisatorisch – und sie können nicht nur den Verein selbst betreffen, sondern auch den Vorstand in seiner Verantwortung:

1. **Vertrauensverlust innerhalb des Vereins**
   Mitglieder, Eltern, Trainer, Ehrenamtliche und Förderer erwarten einen verantwortungsvollen Umgang mit ihren personenbezogenen Daten; fehlt der verantwortungsvolle Umgang, kann das zu Austritten und sinkender Bereitschaft zur Unterstützung führen. Verlorenes Vertrauen lässt sich nur sehr schwer wiederherstellen – und oft deutlich langsamer, als ein Datenschutzproblem entsteht.
2. **Bußgelder durch die Aufsichtsbehörden**
   Unterliegt ein Verein der DSGVO, können Aufsichtsbehörden bei Verstößen nicht nur Nachbesserungen, sondern auch Bußgelder verhängen – unabhängig von der Größe oder Ehrenamtlichkeit des Vereins. Schon einfache Versäumnisse wie unverschlüsselte E-Mail-Kommunikation oder fehlende Einwilligungen können ein Behördenverfahren auslösen.
3. **Schadensersatzansprüche von Betroffenen**
   Betroffene können nach Art. 82 DSGVO Schadensersatz verlangen, wenn ihnen durch einen Datenschutzverstoß ein materieller oder immaterieller Schaden entsteht, beispielsweise durch Veröffentlichung von Fotos oder Kontaktdaten ohne Erlaubnis. Solche Ansprüche werden heute zunehmend aktiv verfolgt – oft auch durch anwaltliche Unterstützung.
4. **Reputationsschäden nach außen**
   Datenschutzvorfälle – etwa veröffentlichte Fotos ohne Einwilligung, öffentlich einsehbare Teilnehmerlisten oder Datenpannen in WhatsApp-Gruppen – können über soziale Medien oder die lokale Presse große Aufmerksamkeit erhalten. Das schadet dem Ruf des Vereins und kann sich negativ auf Sponsoren, Kooperationen oder die Mitgliedergewinnung auswirken.

### Datenschutzverstöße können teuer werden

**Ein Fall: Das Arbeitsgericht Duisburg (Urteil vom 26.9.2024, Az. 3 Ca 77/24) hat entschieden, dass die unzulässige Weitergabe von Gesundheitsdaten eines Vereinsmitarbeiters an die gesamte Vereinsmitgliedschaft einen immateriellen Schadensersatzanspruch von 10.000 € auslöst. Die Vereinspräsidentin informierte in einem Rundschreiben alle Mitglieder über den lang andauernden Krankenstand des Mitarbeiters – ohne seine Zustimmung.**

**Damit lagen eine unzulässige Verarbeitung sensibler Gesundheitsdaten und somit ein eindeutiger Verstoß gegen die DSGVO vor.**

***Hinweis:* Selbst eine Einwilligung wäre hier kritisch zu prüfen, da bei Beschäftigten oft keine echte Freiwilligkeit angenommen werden kann.**

**Besonders praxisrelevant: In dem Verfahren wurde nicht der Verein, sondern die Vereinspräsidentin persönlich haftbar gemacht. Das zeigt deutlich, wie ernst Gerichte Datenschutzverstöße nehmen. Wer sensible Daten ohne Rechtsgrundlage weitergibt, riskiert nicht nur Ärger – sondern ganz konkret persönliche Schadensersatzforderungen gegen Vorstandsmitglieder.**

**Das Beispiel macht deutlich, dass auch Vereine bei Datenschutzfragen dieselben Maßstäbe erfüllen müssen wie Unternehmen – unabhängig von Größe, Ehrenamtlichkeit oder Vereinsstruktur.**

# Selbsttest: Wie datenschutzfit ist Ihr Verein?

**Markieren Sie pro Frage den passenden Wert (0–3). Je höher die Summe, desto besser ist Ihr Datenschutzstatus.**

0 = nein/nicht vorhanden • 1 = teilweise • 2 = weitgehend • 3 = vollständig umgesetzt

| Beschreibung | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| Sie wissen genau, welche personenbezogenen Daten im Verein verarbeitet werden.<br>(Beispiele: Mitgliederliste, Trainerkontakte, Spendenverwaltung, Kontaktformular der Website.) | ○ | ○ | ○ | ○ |
| Für jede Verarbeitung ist eine Rechtsgrundlage (Art. 6 DSGVO) dokumentiert.<br>(Beispiele: Mitgliedsdaten = Vertrag; Spendenquittung = rechtliche Pflicht; Fotos auf Website = Einwilligung.) | ○ | ○ | ○ | ○ |
| Neue Mitglieder erhalten beim Eintritt eine Datenschutzinformation (Art. 13 DSGVO).<br>(Beispiele: Beiblatt zur Beitrittserklärung + Link zur Datenschutzerklärung.) | ○ | ○ | ○ | ○ |
| Einwilligungen werden eingeholt, wenn keine andere Grundlage greift.<br>(Beispiele: Newsletter an Nichtmitglieder; Porträtfotos für Social Media.) | ○ | ○ | ○ | ○ |
| Ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) liegt vor.<br>(Beispiele: Tabelle mit Zweck, Datenkategorien, Empfängern, Löschfristen.) | ○ | ○ | ○ | ○ |
| Mit Dienstleistern bestehen Auftragsverarbeitungsverträge (AVV) (Art. 28 DSGVO).<br>(Beispiele: Vereinssoftware, Newsletter-Tool, Cloud/Webhoster.) | ○ | ○ | ○ | ○ |
| Technische Schutzmaßnahmen sind umgesetzt.<br>(Beispiele: starke Passwörter, 2FA, aktuelle Virensoftware, verschlüsselte Back-ups.) | ○ | ○ | ○ | ○ |
| Organisatorische Regeln existieren und werden beachtet.<br>(Beispiele: BCC bei Rundmails, sichere Ablage von Papierakten.) | ○ | ○ | ○ | ○ |
| Löschfristen existieren und werden eingehalten.<br>(Beispiel: Daten ehemaliger Mitglieder nach Ablauf von Aufbewahrungsfristen löschen.) | ○ | ○ | ○ | ○ |
| Website und Social Media sind geprüft.<br>(Beispiele: Datenschutzhinweise, Consent-Banner falls nötig, Impressum, Umgang mit Fotos.) | ○ | ○ | ○ | ○ |
| Es gibt einen Plan für Datenpannen (72-Stunden-Frist-Prüfung).<br>(Beispiel: Checkliste „Wer wird informiert? Was dokumentieren?“) | ○ | ○ | ○ | ○ |
| Es existiert ein Konzept zur Sensibilisierung von Vereinsmitgliedern, die mit personenbezogenen Daten arbeiten.<br>(Beispiele: jährliche Info-Mail + Merkblatt, Anwesenheitsliste der Schulung.) | ○ | ○ | ○ | ○ |
| Zugriffskonzepte sind definiert („Need to know“).<br>(Beispiele: Nur Kassenwart sieht Bankdaten; Trainer sieht Trainingsliste, nicht Spendenliste.) | ○ | ○ | ○ | ○ |
| Offboarding ist geregelt.<br>(Beispiele: Zugänge entzogen, Datenträger zurückgegeben, Passwörter geändert.) | ○ | ○ | ○ | ○ |
| Datenübermittlungen an Dritte sind transparent und begründet.<br>(Beispiel: Meldung an Dachverband mit klarer Rechtsgrundlage und Minimaldaten.) | ○ | ○ | ○ | ○ |
| Es gibt ein Konzept zur Umsetzung von Betroffenenrechten; insbesondere können Auskunftsansprüche fristgerecht bearbeitet werden. | ○ | ○ | ○ | ○ |
| Private Geräte (BYOD) sind geregelt.<br>(Beispiel: Vereinsdaten nicht auf privaten Geräten.) | ○ | ○ | ○ | ○ |

## Auswertung

| Punkte | Bedeutung |
|---|---|
| 43–51 | Sehr gut: Datenschutz ist im Vereinsalltag verankert. Prozesse funktionieren, nur gelegentlicher Feinschliff nötig. |
| 32–42 | Gut: Stabile Basis vorhanden. Einige Bereiche sollten gezielt verbessert werden, z. B. Löschfristen, AV-Verträge oder Offboarding. |
| 21–31 | Auf dem Weg: Wichtige Elemente fehlen noch. Jetzt strukturiert priorisieren – zuerst Verzeichnis, Informationspflichten, organisatorische Regeln und technische Schutzmaßnahmen. |
| 0–20 | Startphase: Datenschutz steckt noch in den Anfängen. Legen Sie jetzt Zuständigkeiten fest und starten Sie mit den Grundmaßnahmen, um typische Risiken auszuschließen. |

# Schritt 1: Bestandsaufnahme der Datenverarbeitung

**Die Grundlage für eine datenschutzkonforme Umsetzung im Verein ist eine rechtmäßige Verarbeitung personenbezogener Daten. Ob diese bereits gegeben ist – oder ob Daten von Vereinsmitgliedern ohne ausreichende Rechtsgrundlage verarbeitet werden –, lässt sich am zuverlässigsten feststellen, indem Sie eine Bestandsaufnahme durchführen.**

## Überblick über alle Daten schaffen

Im ersten Schritt beginnen Sie mit einer vollständigen Bestandsaufnahme aller personenbezogenen Daten, die in Ihrem Verein verarbeitet werden. Notieren Sie dabei auch jeweils den Zweck der Verarbeitung. Anschließend prüfen Sie, ob für jede einzelne Verarbeitung eine rechtliche Grundlage besteht. Fehlt eine solche Grundlage, ist die Verarbeitung unzulässig; in diesem Fall müssen die Daten umgehend gelöscht oder eine wirksame Einwilligung eingeholt werden. Am besten gelingt das mit einer Tabelle: Sie zeigt auf einen Blick, welche Datenkategorien verarbeitet werden, welchem Zweck sie dienen und ob die erforderliche Rechtsgrundlage vorhanden ist oder ergänzt werden muss.

## Rechtsgrundlage korrekt bestimmen

Für jede Verarbeitung personenbezogener Daten braucht es eine Rechtsgrundlage nach Art. 6 Datenschutz-Grundverordnung (DSGVO). Ohne eine solche Grundlage ist die Nutzung unzulässig – auch wenn die Absicht gut ist oder „man das schon immer so gemacht hat". Gerade Vereine unterschätzen diesen Punkt häufig, was in der Praxis zu unzulässigen Verarbeitungen und teils erheblichen Folgen führen kann.

### Zentrale Regel im Datenschutz:

**keine Verarbeitung ohne Rechtsgrundlage**

Die DSGVO stellt mehrere gesetzliche Rechtsgrundlagen bereit, auf die sich Vereine stützen können. Für jede einzelne Verarbeitung – ob Mitgliederverwaltung, Organisation des Trainingsbetriebs oder Veröffentlichung von Fotos – muss eine geeignete Rechtsgrundlage eindeutig festgelegt werden.

Im Vereinsumfeld werden in der Praxis überwiegend vier gesetzliche Rechtsgrundlagen herangezogen:

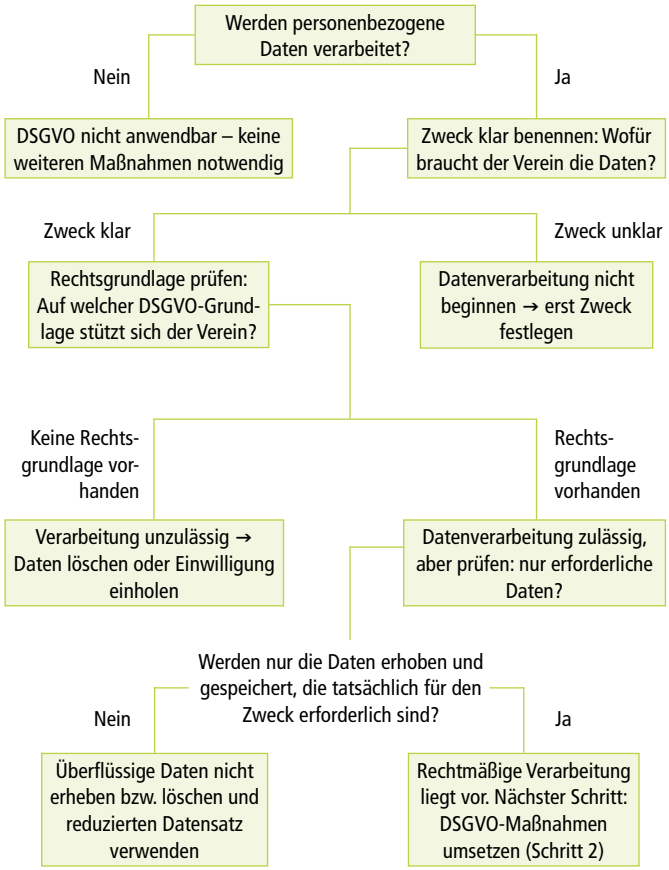
- Vertrag/Mitgliedschaft: Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO
- rechtliche Verpflichtung: Art. 6 Abs. 1 Satz 1 Buchst. c DSGVO
- berechtigtes Interesse: Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO
- Einwilligung: Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO

Eine Einwilligung ist also nicht in jedem Fall erforderlich – jedenfalls dann nicht, wenn bereits eine der anderen Rechtsgrundlagen greift.

Welche Rechtsgrundlage einschlägig ist, richtet sich immer nach dem konkreten Zweck der Verarbeitung. Dieser Zweck muss eindeutig feststehen und nachvollziehbar dokumentiert werden.

| Rechtsgrundlage | Typische Beispiele im Vereinsalltag |
|---|---|
| **Vertrag/Mitgliedschaft – Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO**<br>„Verarbeitung ist zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich." | › Aufnahme eines Mitglieds und Erhebung der Bankverbindung für den Beitragseinzug<br>› Verwaltung von Mitgliedsdaten und Zahlungsabwicklung |
| **Rechtliche Verpflichtung – Art. 6 Abs. 1 Satz 1 Buchst. c DSGVO**<br>„Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt." | › Ausstellen Spendenquittungen und ordnungsgemäße Buchführung<br>› Aufbewahrung von Zahlungsbelegen nach Abgabenordnung und Steuerrecht<br>› Pflichtmeldungen von Mitgliederdaten an Dach-/Sportverbände, wenn satzungsgemäß vorgeschrieben<br>› Einhaltung gesetzlicher Aufbewahrungspflichten (z. B. Vereins-, Steuer- oder Gemeinnützigkeitsrecht) |
| **Berechtigtes Interesse – Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO**<br>„Verarbeitung zur Wahrung berechtigter Interessen, sofern keine überwiegenden Interessen der betroffenen Person entgegenstehen." | › Versand von Einladungen zur Mitgliederversammlung<br>› Vereinsbezogene Informationen an Mitglieder<br>› Teilnehmerlisten für Trainingsgruppen/Kurse<br>› Interne Kommunikation im Verein (z. B. E-Mail/Messenger)<br>› Veröffentlichung von Gruppenfotos oder Vereinsberichten (nach Interessenabwägung – besondere Vorsicht aber bei Kinderfotos: nur mit Einwilligung)<br>› Videoüberwachung des Vereinsheims zur Sicherung vor Vandalismus/Diebstahl (aber strenge Anforderungen: Hinweisschilder, Interessenabwägung, Speicherfristen beachten) |
| **Einwilligung – Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO**<br>„Freiwillig, informiert und unmissverständlich abgegebene Zustimmung zur Verarbeitung personenbezogener Daten." | › Veröffentlichung von Einzelporträts oder Videos einzelner Personen<br>› Newsletter-Versand an Nicht-Mitglieder *(bei Mitgliedern ebenfalls sinnvoll mit informierter Einwilligung)*<br>› Erfassung und Speicherung von Gesundheitsdaten (z. B. Allergien, Verletzungen, Medikamentenbedarf)<br>› Weitergabe von Kontaktdaten an Sponsoren, Presse oder Kooperationspartner<br>› Nutzung von personenbezogenen Daten für Werbung oder Spendenaufrufe |

## Schritt für Schritt: Rechtmäßigkeit der Datenverarbeitung prüfen




## Die Einwilligung als Rechtsgrundlage

Eine der in Art. 6 DSGVO genannten Rechtsgrundlagen ist die Einwilligung. Sie wird immer dann erforderlich, wenn keine der zuvor genannten Rechtsgrundlagen greift oder der Verarbeitungszweck über das für den Vereinsbetrieb Notwendige hinausgeht. Typische Fälle im Vereinsalltag, in denen eine Einwilligung erforderlich ist, betreffen vor allem die Veröffentlichung von Einzelfotos oder Videos einzelner Personen auf der Vereinswebsite, in sozialen Medien oder in der Presse, da hierfür keine andere Rechtsgrundlage besteht.

- Einwilligungsbedürftig ist außerdem der Versand von Newslettern mit Angeboten, Veranstaltungen oder Sponsorenaktionen, soweit diese über die reine Mitgliederinformation hinausgehen.

Soll eine Einwilligung als Rechtsgrundlage dienen, müssen die Anforderungen der Art. 4 Nr. 11 und Art. 7 DSGVO erfüllt sein:

Aktive Willensbekundung – keine vorausgewählten Kästchen, kein Schweigen. Hinweis: Konkludente Einwilligungen sind möglich, der Nachweis ist jedoch deutlich schwieriger.

- Freiwilligkeit – Einwilligung muss ohne Druck erfolgen; Verweigerung darf keine Nachteile haben.
- Koppelungsverbot – Leistungen oder Verträge dürfen nicht von einer Einwilligung abhängig gemacht werden, wenn die Verarbeitung hierfür nicht erforderlich ist.
- Informiertheit – klare Angaben zu Verantwortlichem, Zweck, Datenkategorien und Widerrufsrecht.
- Widerruf jederzeit möglich – er wirkt nur für die Zukunft und muss genauso einfach wie die Einwilligung selbst sein.
- Nachweisbarkeit – Form ist frei, aber eine dokumentierbare Einholung ist erforderlich, um die Erteilung belegen zu können.

### Nicht nur sammeln – sondern im Blick behalten: Consent-Management

**Einwilligungen müssen nicht nur eingeholt, sondern auch nachvollziehbar dokumentiert und verwaltet werden. Wichtig ist zudem ein klares Verfahren, um Widerrufe zu erfassen und die weitere Verarbeitung unverzüglich zu stoppen. Ebenso sollte festgelegt sein, wer im Verein dafür verantwortlich ist. So wird sichergestellt, dass Daten nur so lange verarbeitet werden, wie eine gültige Einwilligung vorliegt.**

Hier finden Sie eine Mustereinwilligungserklärung für die Veröffentlichung von Fotos und/oder Videos sowie für den Versand eines Newsletters.

**MUSTER — Einwilligungserklärung für Vereinsmitglieder**

Einwilligung gemäß Art. 6 Abs. 1 Satz 1 Buchst. a. DSGVO

Der Verein [Name des Vereins] e. V. bittet um Ihre Einwilligung für folgende freiwillige Verarbeitungen personenbezogener Daten. Diese Verarbeitungen sind nicht für die Mitgliedschaft erforderlich und erfolgen nur, wenn Sie ausdrücklich zustimmen.

Ich willige ein, dass – je nach Auswahl – folgende Verarbeitungen erfolgen dürfen: (Bitte Zutreffendes ankreuzen – Mehrfachauswahl möglich)

Fotos/Videos
○ Veröffentlichung von Fotos, auf denen ich erkennbar bin
○ Veröffentlichung von Videos, auf denen ich erkennbar bin

Veröffentlichungsorte (optional einzeln wählbar):
○ Vereinswebsite
○ Social-Media-Kanäle des Vereins
○ Presse/Medienberichte
○ Vereinschronik/Printpublikationen

○ Newsletter/E-Mail-Infos: Ich willige ein, dass mir der Verein Informationen zu Vereinsaktivitäten und Veranstaltungen per E-Mail/Newsletter zusendet.

Widerruf: Diese Einwilligungen sind freiwillig und können jederzeit mit Wirkung für die Zukunft ohne Angabe von Gründen widerrufen werden. Ein Widerruf hat keine Auswirkungen auf die Mitgliedschaft im Verein und keine Nachteile für mich.

Ort, Datum: _____

Unterschrift Mitglied: _____

**Bei Minderjährigen: Unterschriften Erziehungsberechtigte
_____**

Verantwortlicher für die Datenverarbeitung: [Vereinsname, Anschrift, E-Mail-Adresse]

Datenschutzbeauftragter (falls benannt): [Name, Kontaktdaten]

### Besonderheit bei Minderjährigen

**Ist ein Mitglied unter 16 Jahren, muss die Einwilligung von den Sorgeberechtigten unterschrieben werden (Art. 8 Abs. 1 DSGVO): von beiden Elternteilen, wenn sie gemeinsam sorgeberechtigt sind.**

# Schritt 2: Datenschutz absichern und im Vereinsalltag verankern

**Wenn Sie Schritt eins sorgfältig durchgeführt haben, ist im besten Fall sichergestellt, dass personenbezogene Daten überhaupt nur auf einer rechtmäßigen Grundlage verarbeitet werden. Doch damit ist es noch nicht getan: Datenschutz ist kein Sprint, sondern ein Marathon. Die bloße Rechtmäßigkeit der Verarbeitung reicht nicht aus; für wirksamen Datenschutz im Verein braucht es gezielte und dauerhaft verankerte Schutzmaßnahmen.**

## Datenschutz organisatorisch verankern

Im nächsten Schritt geht es daher darum, die Anforderungen der DSGVO in den Vereinsstrukturen umzusetzen, damit die Betroffenenrechte gewahrt bleiben und die erfassten Daten dauerhaft geschützt sind. Dafür braucht es klare Zuständigkeiten, festgelegte Abläufe und eine nachvollziehbare Dokumentation. So wird Datenschutz alltagstauglich und verlässlich gelebt, statt nur auf dem Papier zu bestehen.

Setzen Sie dafür in Ihrem Verein die folgenden Maßnahmen um:

### Maßnahme 1: Verantwortlichkeiten klären

In der Regel ist der Vereinsvorstand für die Einhaltung des Datenschutzes verantwortlich. Er vertritt den Verein nach außen (§ 26 Bürgerliches Gesetzbuch). Bei größeren Vereinen kann zusätzlich ein Datenschutzbeauftragter benannt werden – verpflichtend ist das, wenn z. B. regelmäßig mehr als 20 Personen „ständig mit der automatisierten Verarbeitung von personenbezogenen Daten" beschäftigt sind (§ 38 Abs. 1 Bundesdatenschutzgesetz); auf die Zahl der Mitglieder kommt es hingegen nicht an. Das gilt auch, wenn es sich um Ehrenamtliche handelt, die Mitgliederlisten pflegen oder E-Mails verschicken.

**Beispiel:** Ein Sportverein hat zehn angestellte Trainer und zwölf Ehrenamtliche, die die Mitgliederverwaltung digital führen. Damit sind mehr als 20 Personen regelmäßig mit automatisierter Datenverarbeitung befasst – der Verein muss also einen Datenschutzbeauftragten benennen und dessen Kontaktdaten veröffentlichen (z. B. auf der Website). Zudem müssen die Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde mitgeteilt werden (vgl. Art. 37 Abs. 7 Datenschutz-Grundverordnung (DSGVO)).

**Tipp:** Richten Sie eine zentrale E-Mail-Adresse für Datenschutzfragen ein (z. B. datenschutz@verein.de). So erreichen Fragen immer die richtige Stelle – auch wenn sich Zuständigkeiten ändern.

### Maßnahme 2: Verarbeitungstätigkeiten dokumentieren

Ein solches Verzeichnis ist Pflicht – auch für Vereine. Es listet alle Prozesse auf, bei denen personenbezogene Daten verarbeitet werden: wofür, auf welcher Grundlage, wie lange und wer Zugriff hat. Diese Übersicht hilft nicht nur bei internen Abläufen, sondern auch im Fall einer Anfrage durch die Aufsichtsbehörde.

**Tipp:** Nutzen Sie hierfür als Grundlage die Tabelle aus Schritt 1 – digital oder auf Papier – folgende Punkte müssen enthalten sein:

- Zweck der Verarbeitung (z. B. Mitgliederverwaltung, Spendenverwaltung, Website)
- betroffene Personengruppen (Mitglieder, Spender, Ehrenamtliche)
- Datenkategorien (Name, Adresse, Kontodaten usw.)
- Empfänger (z. B. Banken, Dachverband, IT-Dienstleister)
- Speicherdauer und Löschfristen
- technische und organisatorische Maßnahmen (z. B. Passwortschutz, Zugriffsbeschränkung)

**Beispiel:** Bei der Mitgliederverwaltung werden Name, Anschrift, Geburtsdatum, E-Mail-Adresse und Bankverbindung verarbeitet. Zweck ist die Verwaltung der Mitgliedschaft und der Beitragseinzug. Dazu haben ausschließlich Vorstand und Mitgliederverwaltung Zugriff. Die Daten werden nach Austritt gemäß Satzung und steuerlichen Aufbewahrungsfristen gelöscht. Dieser Vorgang wird als eigener Eintrag im Verzeichnis geführt.

Ebenso entsteht ein eigener Eintrag z. B. für

- den Versand des Vereins-Newsletters,
- die Verwaltung von Spenden und
- die Veröffentlichung auf der Vereinswebsite (z. B. Fotos, Kontaktdaten von Funktionsträgern).

### Maßnahme 3: Informationspflichten erfüllen

Transparenz ist einer der wichtigsten Grundsätze der DSGVO. Mitglieder, Spender und Ehrenamtliche müssen wissen, welche Daten verarbeitet werden, zu welchem Zweck und welche Rechte sie haben. Je verständlicher und kürzer die Hinweise formuliert sind, desto leichter werden sie akzeptiert und tatsächlich gelesen.

Das gelingt am einfachsten mit klaren Informationsblättern:

- bei Aufnahme neuer Mitglieder (Beitrittsformular und Datenschutzhinweis),
- auf der Vereinswebsite (Datenschutzhinweise),
- bei Veranstaltungen oder Fotoaktionen (Hinweisschilder oder Flyer).

**Beispiel:** Beim Spendenlauf erhalten Teilnehmende am Anmeldestand ein kurzes Infoblatt mit diesem Text: „Wir verarbeiten euren Namen und eure Kontaktdaten zur Organisation des Laufs und zur Ausstellung der Teilnahmebestätigung. Die Daten werden nach Abschluss der Veranstaltung gemäß unseren Aufbewahrungsfristen gelöscht."

**Hinweis:** Entscheidend ist nicht die Länge, sondern dass alle nach Art. 13 DSGVO erforderlichen Angaben enthalten sind.

## Maßnahme 4: Technische und organisatorische Maßnahmen (TOMs)

Technik allein genügt nicht – und organisatorische Regeln ohne technische Absicherung ebenso wenig. Erst das Zusammenspiel beider Bereiche macht Datenschutz belastbar.

Technische Basisschutzmaßnahmen (Pflichtprogramm):

- starke, individuelle Passwörter und Zwei-Faktor-Authentifizierung
- regelmäßige Datensicherungen inklusive Rücksicherungstest
- klar geregelte Zugriffsrechte nach dem Need-to-know-Prinzip
- aktuelle Systeme, Virenschutz und Sicherheitsupdates
- Geräte- und Cloudschutz (Verschlüsselung, Sperrbildschirm, kein Zugriff ohne Authentifizierung)

Organisatorische Basisschutzmaßnahmen (genauso wichtig):

- sensible Daten niemals über WhatsApp oder unverschlüsselte E-Mails weiterleiten
- Papierunterlagen und Listen mit Mitgliederdaten nur unter Verschluss
- alte Unterlagen und Datenträger datensicher entsorgen (z. B. Aktenvernichter)
- Auftragsverarbeitungsverträge (AVV) mit Software-, Cloud- und Newsletter-Diensten abschließen – auch bei kostenlosen Tools

## Maßnahme 5: Verträge mit Dritten prüfen

Sobald externe Dienstleister personenbezogene Daten für den Verein verarbeiten – etwa Webhoster, Buchhaltungsservice, Cloudanbieter oder Vereinssoftware –, muss ein AVV nach Art. 28 DSGVO geschlossen werden.

*Wichtig:* Ein fehlender, unvollständiger oder fehlerhafter AVV kann Sanktionen und Bußgelder nach sich ziehen.

Dieser Vertrag regelt,

- welche Daten verarbeitet werden dürfen,
- zu welchem Zweck,
- welche Sicherheitsmaßnahmen der Dienstleister einsetzt und
- dass er die Daten nicht für eigene Zwecke nutzt.

**Tipp:** Viele Anbieter stellen standardisierte AVV bereit, die Sie nur noch unterzeichnen müssen. Prüfen Sie trotzdem, ob die wesentlichen Punkte – etwa Löschfristen, Unterauftragnehmer oder Sicherheitsmaßnahmen – enthalten sind.

## Maßnahme 6: Dokumentation und Nachweis

Die DSGVO verlangt, dass Sie nachweisen können, welche Datenschutzmaßnahmen umgesetzt wurden. Das muss kein kompliziertes Handbuch sein – eine einfache Sammelmappe oder ein digitaler Ordner genügt.

Dokumentieren Sie z. B.,

- wann Einwilligungen eingeholt wurden,
- wann Informationspflichten aktualisiert wurden,
- wann Systeme überprüft oder Passwörter geändert wurden und
- wann eine Schulung oder Sensibilisierung stattgefunden hat.

**Beispiel:** Ein Verein führt einmal jährlich eine kurze Überprüfung durch und hält die Ergebnisse in einem Dokument fest – z. B. so:

15.1.2026 – Passwörter für E-Mail-Konten aktualisiert

20.2.2026 – AVV mit Cloudanbieter geprüft

1.3.2026 – Datenschutzhinweise Beitrittsformular aktualisiert

Das Dokument wird im Datenschutzordner abgelegt. So kann der Verein jederzeit nachweisen, welche Maßnahmen umgesetzt wurden, und erfüllt damit zugleich seine Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

## Checkliste: So setzen Sie Datenschutz im Verein richtig um

| Prüffrage | Hintergrund | In Ordnung? |
|---|---|---|
| Verantwortlichkeiten geregelt? | › Der Vorstand trägt die Gesamtverantwortung. Eine Ansprechperson für Datenschutzfragen ist benannt, damit Rückfragen und Aufgaben nicht „anonym" bleiben. | ○ Ja ○ Nein |
| Datenschutzbeauftragter bestellt (falls nötig)? | Pflicht ab 20 Personen, die regelmäßig personenbezogene Daten verarbeiten – auch wenn es Ehrenamtliche sind. | ○ Ja ○ Nein |
| Verzeichnis der Verarbeitungstätigkeiten vorhanden? | Alle Prozesse mit personenbezogenen Daten sind dokumentiert (Mitglieder, Spenden, Website etc.) – dadurch wird die Verarbeitung nachvollziehbar und prüfbar. | ○ Ja ○ Nein |
| Informationspflichten erfüllt? | Datenschutzerklärung an Mitglieder ausgehändigt und auf Website veröffentlicht, damit Betroffene jederzeit wissen, welche Daten zu welchem Zweck verarbeitet werden. | ○ Ja ○ Nein |
| AVV abgeschlossen? | Mit externen Dienstleistern (z. B. Cloudanbieter, Vereinssoftware, Webhoster) wurden AVV geschlossen – sie regeln, wie der Dienstleister Datenschutz sicherstellt. | ○ Ja ○ Nein |
| TOMs umgesetzt? | Passwortschutz, Zugriffsbeschränkungen, regelmäßige Back-ups und Updates sind gewährleistet, um unbefugten Zugriff und Datenverlust zu verhindern. | ○ Ja ○ Nein |
| Organisatorische Regeln vorhanden? | Datenschutzregeln für E-Mail, WhatsApp, Papierakten und Datenträger wurden festgelegt, damit alle Beteiligten sicher und einheitlich handeln. | ○ Ja ○ Nein |
| Löschfristen definiert und umgesetzt? | Veraltete oder nicht mehr benötigte Daten werden regelmäßig gelöscht, damit keine „Altbestände" mit unnötigen Risiken bestehen bleiben. | ○ Ja ○ Nein |
| Schulungen und Merkblätter verteilt? | Ehrenamtliche und Vorstandsmitglieder wissen, wie sie mit personenbezogenen Daten umgehen – auch ohne IT-Vorkenntnisse. | ○ Ja ○ Nein |

# 8 typische Datenschutzfehler – und wie Sie sie vermeiden

**Im Vereinsbetrieb passieren Datenschutzfehler oft nebenbei und ohne böse Absicht. Die folgenden Beispiele zeigen, wo es regelmäßig hakt – und wie Sie es direkt besser machen.**

## Fehler 1: Der offene E-Mail-Verteiler

Einladung zur Jahreshauptversammlung – und alle Adressen stehen im „An"-Feld. So können sämtliche Mitglieder die privaten E-Mail-Adressen der anderen sehen.

So geht's besser:

Immer den BCC-Verteiler („Blindkopie") nutzen oder ein professionelles Newsletter-Tool einsetzen, das den Versand automatisch datenschutzkonform abwickelt.

## Fehler 2: WhatsApp-Gruppe für Trainer und Eltern

Aus organisatorischen Gründen richten viele Trainer WhatsApp-Gruppen ein, um Termine oder Informationen zu teilen. Doch WhatsApp übermittelt Daten wie Telefonnummern an Server außerhalb der EU. Das ist ohne Einwilligung problematisch.

So gelingt es ohne Datenschutzrisiko:

Am besten auf datenschutzfreundlichere Tools umsteigen – etwa Signal, Threema oder spezielle Vereins-Apps. Wenn WhatsApp unvermeidbar ist, sollten alle Beteiligten ausdrücklich einwilligen. Zudem muss sichergestellt sein, dass niemand benachteiligt wird, wenn er WhatsApp nicht nutzen möchte.

## Fehler 3: Fotos im Gruppenchat

Nach dem Turnier landet ein Gruppenfoto direkt im Chat. Schnell leiten Eltern es weiter oder posten es in Statusmeldungen – ohne dass jemand daran denkt, dass es Kinder betrifft.

Empfohlene Vorgehensweise:

Fotos nicht über Messenger-Dienste teilen, sondern über passwortgeschützte Vereinsclouds oder direkt über den Vereinsaccount veröffentlichen – und nur, wenn eine Einwilligung vorliegt. Einmal veröffentlichte Fotos lassen sich kaum zurückholen. Lieber ein Bild weniger als eine Einwilligung zu wenig. Denn einmal geteilt, kann sich ein Foto schnell völlig unkontrolliert weiterverbreiten.

## Fehler 4: Teilnehmerlisten und Aushänge

Bei Wettkämpfen oder Ferienfreizeiten hängen Teilnehmerlisten mit Namen, Geburtsdatum und Telefonnummern öffentlich aus. Jeder Besucher kann die Daten einsehen oder fotografieren.

Korrekte Umsetzung:

Aushänge nur intern zugänglich machen, etwa in Vereinsräumen. Wenn Listen öffentlich nötig sind, z. B. bei Startnummern, dann nur Vornamen oder Pseudonyme verwenden. Gesundheits- oder Kontaktdaten gehören nie auf öffentliche Aushänge.

## Fehler 5: Fotos in der Presse oder auf der Website

Der Verein schickt Veranstaltungsfotos an die Lokalzeitung – ohne vorherige Einwilligung. Später beschweren sich Betroffene, weil sie mit vollem Namen veröffentlicht wurden.

So geht's richtig:

Vor dem Versand immer prüfen, ob eine Einwilligung vorliegt und ob das Bild der Berichterstattung über ein öffentliches Ereignis dient. Ist die Person nur Beiwerk oder im Mittelpunkt? Pressearbeit ist wichtig – aber immer mit Respekt vor der Privatsphäre.

## Fehler 6: Alte Datenbestände

Im Schrank stapeln sich alte Listen, Foto-CDs und Gesundheitsdaten früherer Jugendfreizeiten. „Kann man ja mal brauchen", denkt man – aber das ist unzulässig.

So macht es Ihr Verein korrekt:

Regelmäßig Datenbereinigung durchführen. Mitgliedsdaten sollten nach Austritt und Ablauf gesetzlicher Fristen gelöscht werden. Ideal ist eine jährliche „Löschwoche" im Verein.

## Fehler 7: Gemeinsame Log-in-Daten für mehrere Personen

Für das Vereins-E-Mail-Postfach oder die Cloud gibt es nur ein einziges Passwort – alle Trainer, Betreuer oder Vorstandsmitglieder nutzen denselben Zugang. Eine personenbezogene Zuordnung ist nicht möglich, wer wann auf welche Daten zugegriffen hat.

Rechtssichere Umsetzung:

Jede Person, die auf personenbezogene Daten zugreift, benötigt einen eigenen Account und ein eigenes Passwort. Zugänge ehemaliger Funktionsträger sofort deaktivieren. Passwörter niemals teilen – auch nicht „nur kurz für die Vertretung".

## Fehler 8: Unbedachte Weitergabe von Kontaktdaten

Eltern oder Mitglieder fragen nach Telefonnummern, um Fahrgemeinschaften oder Trainingsabsprachen zu organisieren – und der Verein leitet die Kontaktdaten einfach weiter. Auch gut gemeint ist das rechtswidrig.

Empfohlene Vorgehensweise:

Kontaktdaten niemals ohne Einwilligung weitergeben. Stattdessen eine kurze Nachricht an die betroffene Person senden: „XY möchte Sie kontaktieren – wenn Sie einverstanden sind, melden Sie sich bitte direkt."

PROFITIEREN SIE VON DEN DIGITALEN ARBEITSHILFEN

# PRIVACYXPERTS – neuer Onlinebereich

**Den gesamten Inhalt von „Datenschutz aktuell“ stellen wir Ihnen auch online zur Verfügung.**
Schauen Sie einfach unter **www.privacyxperts.de**

**QR-Code scannen und loslegen!**

## Ihre Vorteile im Überblick:

Ihr Onlinebereich bietet Ihnen alle Ausgaben und Beiträge auf einen Klick sowie zahlreiche Muster und Vorlagen zum praktischen Sofort-Download.

### Alle Inhalte auf einen Blick!

Lassen Sie sich alle bisher erschienenen Ausgaben online anzeigen. Wählen Sie die gewünschten Inhalte – Ausgaben, Beiträge und Muster-Vorlagen. Laden Sie sich diese herunter oder lesen und nutzen Sie sie gleich online.



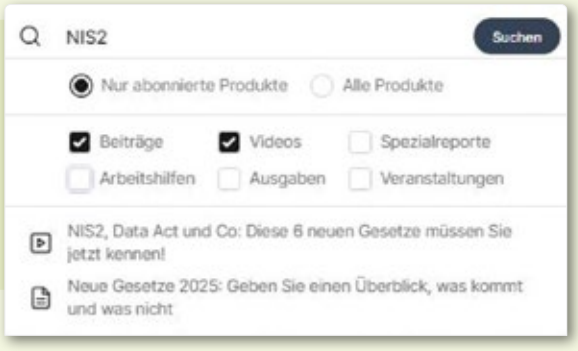
### Tipp:

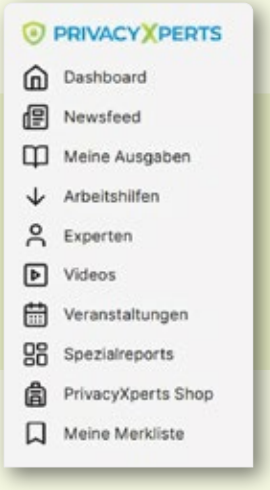
Setzen Sie die für Sie wichtigsten Ausgaben, Beiträge und Arbeitshilfen auf Ihre Merkliste. So haben Sie Ihre TOP-Themen immer schnell im Blick.

### Praktische Suchfunktion!

Sie suchen nach etwas Bestimmtem – beispielsweise Informationen über das Thema NIS2?

Geben Sie Ihren Suchbegriff in das Suchfeld ein und wählen Sie das gewünschte Format.




### Erkunden Sie Ihren Onlinebereich ...

... und entdecken Sie viele weitere, nützliche, hilfreiche und interessante Inhalte und Inklusivleistungen, die Ihren Fachratgeber optimal ergänzen. Viel Erfolg!

**Telefon: 02 28 95 50 150**
**Fax: 02 28 36 96 480**
**E-Mail: kundendienst@privacyxperts.de**
**Internet: www.privacyxperts.de**

**Ein Unternehmensbereich des VNR Verlags**
**für die Deutsche Wirtschaft AG**
**Theodor-Heuss-Straße 2–4**
**53177 Bonn**