



TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Wie der Verein Daten tatsächlich schützt

ART. 24, ART. 32 DSGVO

ENTWURF – INTERNES DOKUMENT

Art. 32 DSGVO verlangt Maßnahmen, die dem Risiko angemessen sind. Für einen ehrenamtlich geführten Verein heißt das nicht Serverraum und Zertifizierung, sondern: abschließbarer Schrank, Passwörter, klare Zuständigkeiten. Was hier steht, muss der Verein aber auch tun — ein Papier, das nicht gelebt wird, schützt niemanden.

1 ZUTRIITTSKONTROLLE — WER INS GEBÄUDE DARF

- Papierunterlagen mit Mitgliederdaten werden in einem abschließbaren Schrank aufbewahrt. Schlüssel haben nur Vorstandsmitglieder.
- Unterlagen werden nicht in privaten Wohnungen gelagert, außer bei der Schriftführung und dem Schatzmeister für die laufende Arbeit; auch dort verschlossen.
- Bei Veranstaltungen werden ausgefüllte Anträge und Listen nicht unbeaufsichtigt liegen gelassen und noch am selben Tag an die zuständige Person übergeben.

2 ZUGANGSKONTROLLE — WER AN DIE SYSTEME DARF

- Jedes Gerät, auf dem Vereinsdaten verarbeitet werden, ist durch Passwort oder biometrisch gesichert und sperrt sich nach spätestens fünf Minuten Inaktivität automatisch.
- Für Vereinskonto werden eigene, nicht anderweitig genutzte Passwörter verwendet. Wo verfügbar, ist Zwei-Faktor-Authentifizierung aktiviert — verbindlich für E-Mail-Postfach, Onlinebanking und die Verwaltung der Internetseite.
- Zugangsdaten werden nicht per E-Mail, Chat oder auf Zetteln weitergegeben, sondern über einen Passwortmanager oder mündlich.
- Es gibt keine gemeinsam genutzten Sammelkonten für mehrere Personen, außer dem allgemeinen Vereinspostfach.

3 ZUGRIFFSKONTROLLE — WER WELCHE DATEN SEHEN DARF

ROLLE	ZUGRIFF
1. und 2. Vorsitz	Mitgliederliste, Protokolle, Korrespondenz
Schatzmeister	zusätzlich Zahlungsdaten, Buchhaltung, Bankzugang
Schriftführung	Mitgliederverwaltung, Verteiler, Protokolle
Kassenprüfer	während der Prüfung Einsicht in Buchhaltung und Belege
Arbeitskreisleitung	nur Teilnehmerlisten des eigenen Arbeitskreises
Sonstige Mitglieder	kein Zugriff

Beim Ausscheiden aus einem Amt werden Zugänge innerhalb einer Woche entzogen und Passwörter geändert. Der Vorstand hält das im Protokoll fest.

4 WEITERGABEKONTROLLE — DATEN UNTERWEGS

- Die Internetseite wird ausschließlich über HTTPS ausgeliefert; Formulardaten werden verschlüsselt übertragen.
- Rundmails an mehrere Empfänger gehen ausnahmslos über BCC oder den Verteilerdienst.
- Mitgliederlisten werden nicht per unverschlüsselter E-Mail verschickt. Ist eine Übermittlung nötig, erfolgt sie passwortgeschützt, wobei das Passwort über einen anderen Kanal mitgeteilt wird.
- Für jeden Dienstleister mit Datenzugriff wird vor Inbetriebnahme ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO geschlossen.

5 EINGABEKONTROLLE — NACHVOLLZIEHEN, WER WAS GEÄNDERT HAT

- Änderungen an der Mitgliederliste werden mit Datum und bearbeitender Person festgehalten.
- Beschlüsse des Vorstands werden fortlaufend nummeriert protokolliert.
- Buchungen werden nicht gelöscht, sondern storniert; der ursprüngliche Vorgang bleibt erkennbar.

6 VERFÜGBARKEIT UND BELASTBARKEIT

- Von Mitgliederliste und Buchhaltung wird **mindestens monatlich** eine Sicherung erstellt und getrennt vom Arbeitsgerät aufbewahrt.
- Mindestens einmal jährlich wird geprüft, ob sich eine Sicherung tatsächlich wiederherstellen lässt. Eine nie getestete Sicherung ist keine Sicherung.
- Zugangsdaten zu allen Vereinskontoen sind so hinterlegt, dass mindestens zwei Vorstandsmitglieder herankommen. Der Verein darf nicht handlungsunfähig werden, wenn eine Person ausfällt.

7 TRENNUNG UND ZWECKBINDUNG

- Vereinsdaten werden von privaten Daten getrennt gehalten: eigenes Postfach, eigener Ordner, eigene Ablage.
- Daten aus Kontaktanfragen werden nicht in die Mitgliederverwaltung übernommen, solange keine Mitgliedschaft entsteht.
- Nachweise zur Beitragsermäßigung werden nur eingesehen, nicht kopiert.

8 LÖSCHUNG

- Einmal jährlich prüft die Schriftführung, welche Daten zu löschen sind, und hält die Prüfung fest.
- Papier mit personenbezogenen Daten wird geschreddert, nicht in den Papierkorb gegeben.
- Datenträger werden vor der Weitergabe oder Entsorgung sicher gelöscht oder zerstört.

9 UMGANG MIT DATENPANNEN

1. Wer eine Panne bemerkt, meldet sie sofort dem Vorstand — ohne Rücksicht auf eigene Fehler.
2. Der Vorstand dokumentiert Zeitpunkt, betroffene Daten, betroffene Personen, wahrscheinliche Folgen und ergriffene Maßnahmen.
3. Besteht ein Risiko für die Rechte der Betroffenen, meldet der Vorstand den Vorfall **innerhalb von 72 Stunden ab Kenntnis** der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (Art. 33 DSGVO).
4. Bei hohem Risiko werden zusätzlich die Betroffenen unverzüglich informiert (Art. 34 DSGVO).
5. Jede Panne wird dokumentiert, auch wenn sie nicht meldepflichtig war.

10 SCHULUNG UND ÜBERPRÜFUNG

- Neue Amtsträger werden vor dem ersten Datenzugriff eingewiesen und auf Vertraulichkeit verpflichtet.
- Der Vorstand überprüft diese Maßnahmen einmal jährlich auf Wirksamkeit und hält das Ergebnis fest.

In Kraft gesetzt am _____

Letzte Überprüfung am _____

Verantwortlich _____