Voraussetzungen nach DSGVO

Die DSGVO ist im Grunde sehr einfach aufgebaut. Denn grundsätzlich ist **JEDE** Verarbeitung von personenbeziehbaren Daten verboten – sofern Sie nicht ERLAUBT ist. Die für Vereine wichtigsten Erlaubnisgrundlagen finden sich in Art. 6 Abs. 1 DSGVO.

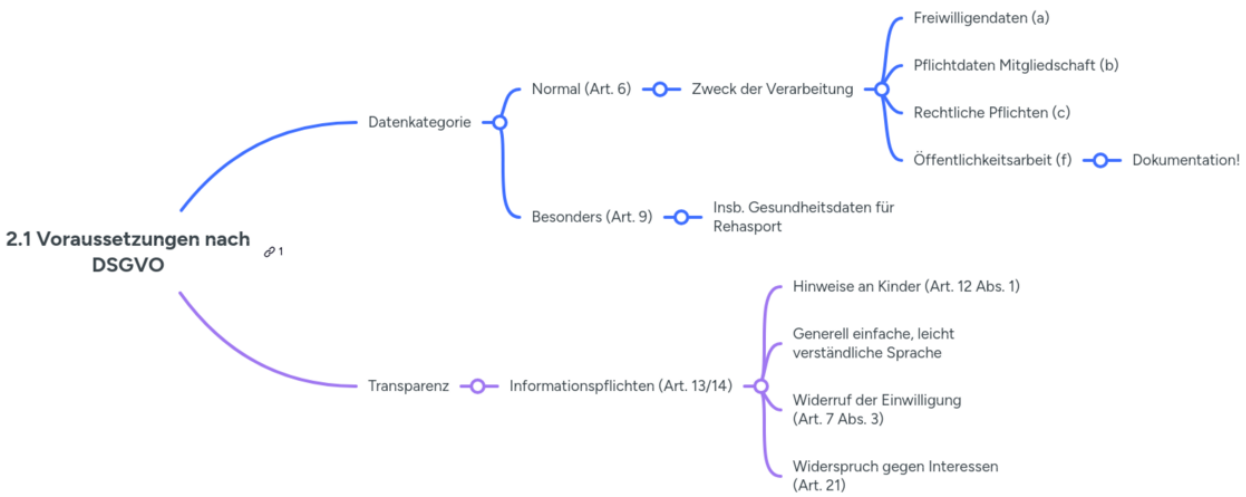
So ist bspw. für die Verarbeitung der Daten im Mitgliedschaftsverhältnis Art. 6 Abs. 1 b) die korrekte Rechtsgrundlage für alle Pflichtdaten. Für die Verarbeitung von zusätzlichen „Freiwilligendaten“ kommen insb. die Einwilligung nach Art. 6 Abs. 1 a) und das berechtigte Interesse nach Art. 6 Abs. 1 f) in Betracht.

Für die Datenverarbeitung im Verein empfiehlt es sich eine **Datenschutzordnung** zu erlassen. Nutzen Sie dafür das entsprechende Muster einer Datenschutzverordnung im Sportverein des LSB NRW.

Welche Rechtsgrundlage ist nun die richtige für mich?

Pauschal lässt sich das nicht beantworten, grundsätzlich sollten wenn möglich andere Erlaubnisgrundlagen genutzt werden als die Einwilligung. Grund dafür ist, dass die Einwilligung jederzeit auch ohne gewichtige Gründe **widerrufen** werden kann. Wenn der Verein aber z.B. die Ablichtung auf Fotos von Sportveranstaltungen stattdessen auf sein **berechtigtes Interesse** an der Berichterstattung seiner Vereinsarbeit stützt, kann hiergegen durch die Betroffenen "nur" widersprochen werden.

WICHTIG: Nach der Rechtsprechung ist **kein „Auffanggrund“** zulässig! Das bedeutet, das der Verein sich vorab für eine einzige der beiden Alternativen entscheiden muss. Ein „**Sicherheitsnetz**“ im Sinne „entweder Einwilligung oder Interesse – später wird man sehen“ ist **unzulässig**. Je nach Mitgliederanzahl, geplanten Zwecken und Alter der abgebildeten macht es Sinn, eine individuelle Regelung für euren Verein zu treffen. Ergänzend ist ratsam, bei Nutzung des berechtigten Interesses die Betroffenen vor Veröffentlichung mündlich zu fragen, ob eine Abbildung in diesem Kontext für Sie in Ordnung ist. Zumeist ist das der Fall, wodurch Probleme vorab verhindert werden. In den seltenen Fällen, wo dies nicht der Fall ist, sollte dann eine **Anonymisierung** des entsprechenden Gesichts mit einem Bildbearbeitungsprogramm erfolgen. Weiteres dazu findet Ihr unter "5. Bildrechte & Videoüberwachung".

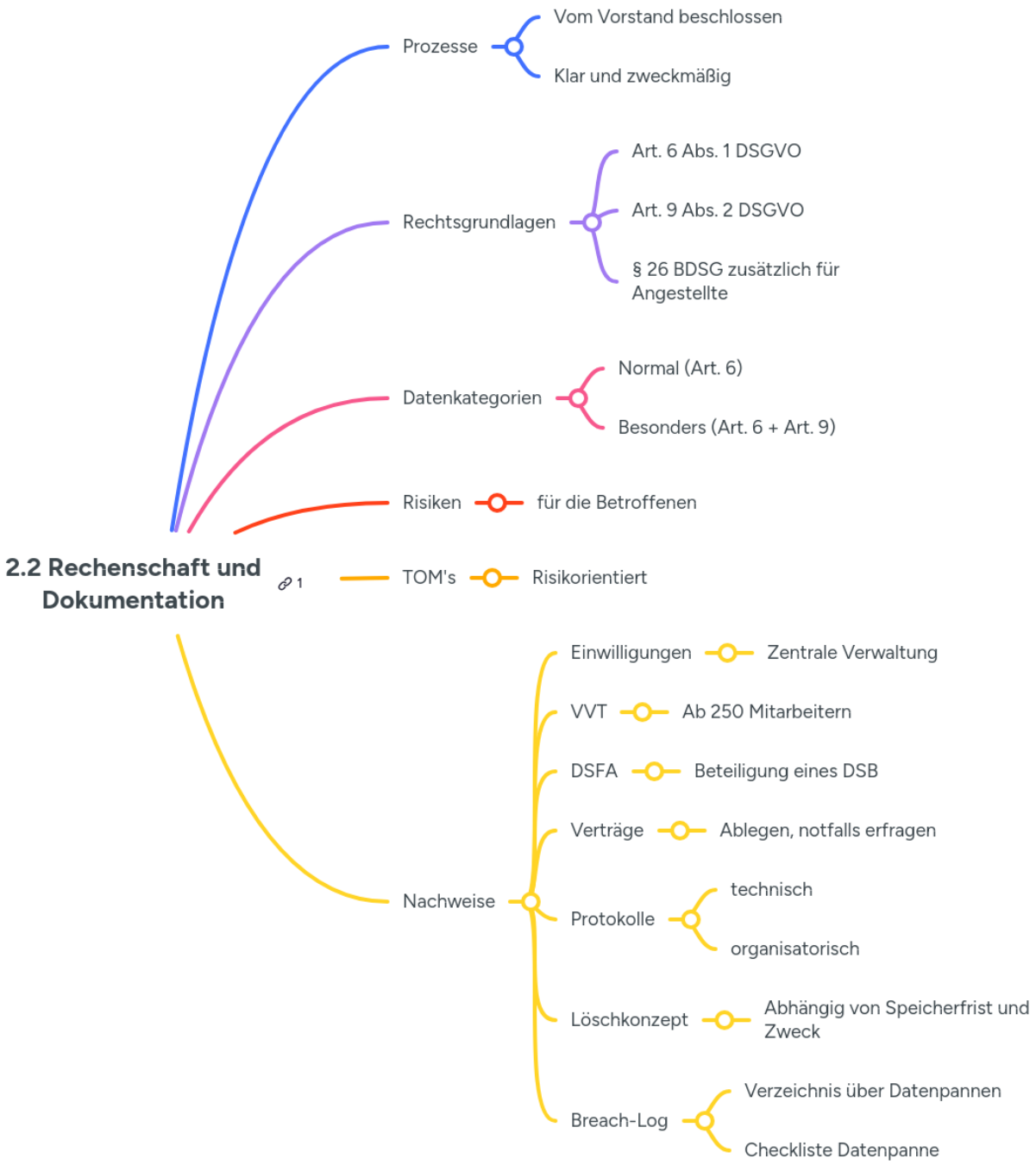


Rechenschaftspflicht und Dokumentation

Jeder Sportverein ist nach der DSGVO verpflichtet, die Einhaltung der Vorgaben nicht nur umzusetzen, sondern auch gem. Art. 5 Abs. 2 DSGVO **nachweisen** zu können. Diese sogenannte **Rechenschaftspflicht** bedeutet, dass der Verein jederzeit belegen muss, wie personenbezogene Daten verarbeitet werden und **welche Maßnahmen** hierfür ergriffen wurden. Dazu gehört insbesondere die Dokumentation aller relevanten Prozesse. Je nach Größe und Umfang der Datenverarbeitung kann auch das Führen eines **Verzeichnisses der Verarbeitungstätigkeiten** (VVT), in dem festgehalten wird, welche Daten zu welchem Zweck verarbeitet werden, erforderlich sein.

Auch **Einwilligungen**, Datenschutz-Folgenabschätzungen (DSFA) bei besonders Eingriffsintensiven Maßnahmen oder die Bearbeitung von Anfragen Betroffener sollten nachvollziehbar dokumentiert werden. Die Dokumentation wird insbesondere bei jur. Auseinandersetzungen und ggü. **Aufsichtsbehörden** relevant. Die interne Dokumentation eines sog. Breaches, also einer **Datenpanne** (Sachverhalt, Auswirkungen, Abhilfe) sollte stets erfolgen. Weiteres dazu findet ihr unter Punkt 4 "Erste Hilfe bei Datenpannen".

Beispiel: Ein besonders großer Verein mit **über 250 Beschäftigten** führt ein Mitgliederverzeichnis (Name, Geburtsdatum, Kontaktdaten). Im VVT sind Zweck (hier die Mitgliederverwaltung), Rechtsgrundlage, Empfänger, Löschfristen, Drittlandtransfers und TOMs dokumentiert. Zugriffsberechtigungen sind festgelegt, „Breaches“ werden nach Art. 33 Abs. 5 dokumentiert und ggf. gemeldet.


2.2 Rechenschaft und Dokumentation
1
Prozesse
Vom Vorstand beschlossen
Klar und zweckmäßig
Rechtsgrundlagen
Art. 6 Abs. 1 DSGVO
Art. 9 Abs. 2 DSGVO
§ 26 BDSG zusätzlich für Angestellte
Datenkategorien
Normal (Art. 6)
Besonders (Art. 6 + Art. 9)
Risiken
für die Betroffenen
TOM's
Risikorientiert
Nachweise
Einwilligungen
Zentrale Verwaltung
VVT
Ab 250 Mitarbeitern
DSFA
Beteiligung eines DSB
Verträge
Ablegen, notfalls erfragen
Protokolle
technisch
organisatorisch
Löschkonzept
Abhängig von Speicherfrist und Zweck
Breach-Log
Verzeichnis über Datenpannen
Checkliste Datenpanne

Betroffenenrechte

Mitglieder und andere betroffene Personen haben verschiedene Rechte gegenüber dem Verein. Dazu zählen insbesondere das Recht auf Auskunft, Berichtigung, Löschung („Recht auf Vergessenwerden“), Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch gegen bestimmte Verarbeitungen. Der Verein muss sicherstellen, dass diese Rechte umgesetzt werden können und Anfragen zügig, in der Regel **innerhalb eines Monats**, beantwortet werden.

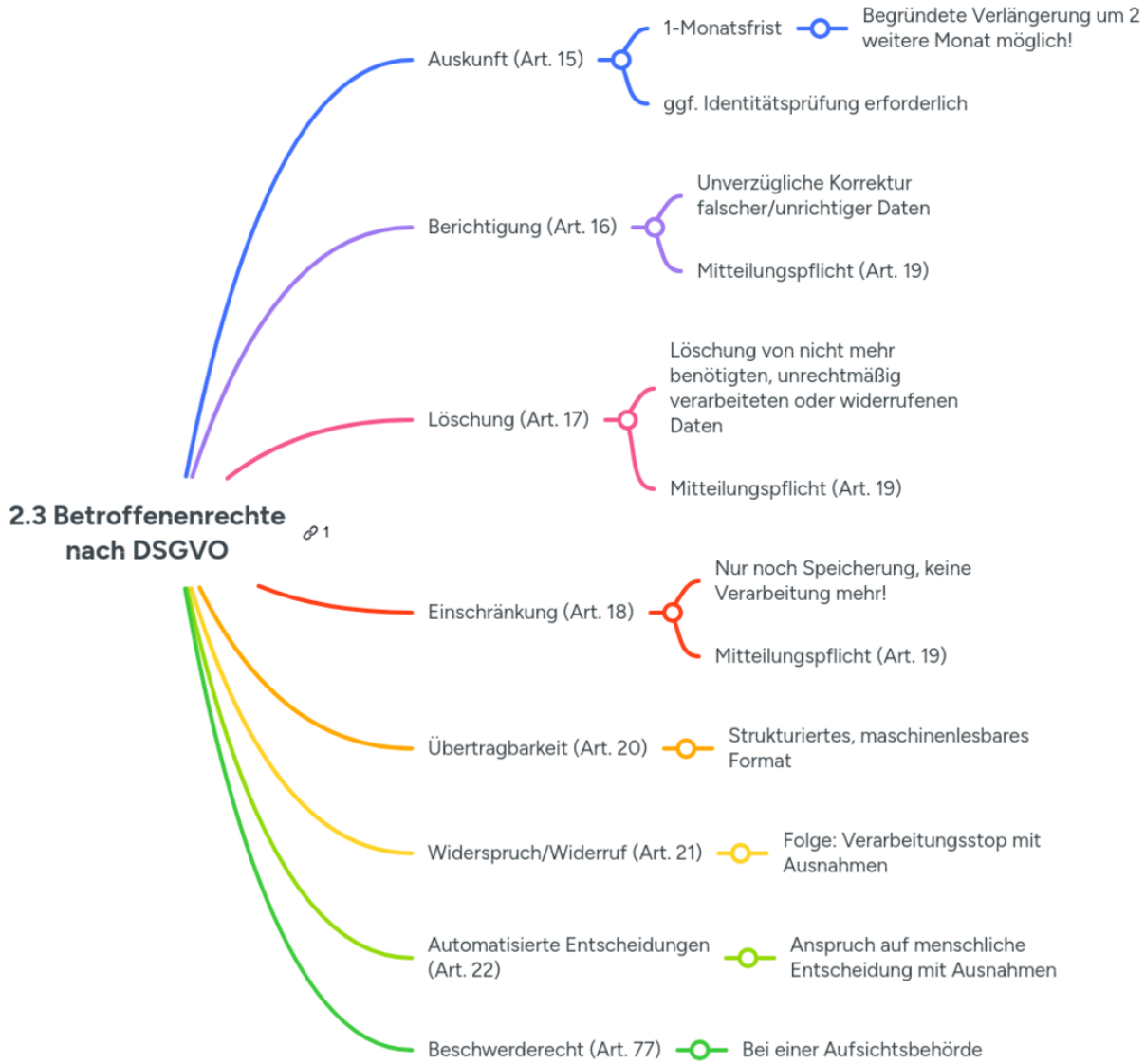
Für die Beantwortung könnt ihr die Vorlage “**Musterschreiben Auskunftsverlangen gemäß Artikel 15 DSGVO**” des LSB NRW nutzen.

Beispiel

Beispiel

Ein Mitglied fragt per E-Mail gem. Art. 15 DSGVO an, welche Daten der Verein über ihn gespeichert hat. Der Verein prüft die Anfrage und gibt innerhalb eines Monats eine Auskunft über die gespeicherten Daten. Das Mitglied verlangt anschließend die Löschung einiger Freiwilligendaten, die der Verein mittels Einwilligung erhoben hat.

Solltet Ihr eine solche Auskunftsanfrage erhalten, könnt ihr euch gerne auch mit dem LSB NRW in Verbindung setzen. Abhängig von eurer IT-Landschaft (Mitgliederverwaltung, E?Mail, Cloud-Dienste) kann die **Datenerhebung für Auskunft und Löschung aufwendig sein**. Richtlinien/Prozesse mit klaren Zuständigkeiten, Vertretungsregelungen, Vorlagen und Fristen helfen (z.B. zentrale Anlaufstelle für Datenschutz und IT im Verein).



Technische und organisatorische Maßnahmen (TOMs)

Um die **Sicherheit** der personenbezogenen Daten zu gewährleisten, müssen Vereine gem. Art. 24 DSGVO geeignete technische und organisatorische Maßnahmen (TOMs) umsetzen, regelmäßig überprüfen und bei Bedarf aktualisieren. Die Maßnahmen müssen **risikobasiert** sein: je sensibler die Daten und je höher Eintrittswahrscheinlichkeit/Schwere möglicher Beeinträchtigungen, desto höher die

Anforderungen. Dazu zählen z. B. der **Schutz vor unbefugtem Zugriff** (Passwortschutz, verschlossene Schränke), **regelmäßige Backups**, die Schulung der Mitarbeitenden und **klare Regelungen**, wer auf welche Daten wann zugreifen darf. Die TOMs und ihre Angemessenheit sind im VVT zu dokumentieren, sofern dieses zu führen ist.

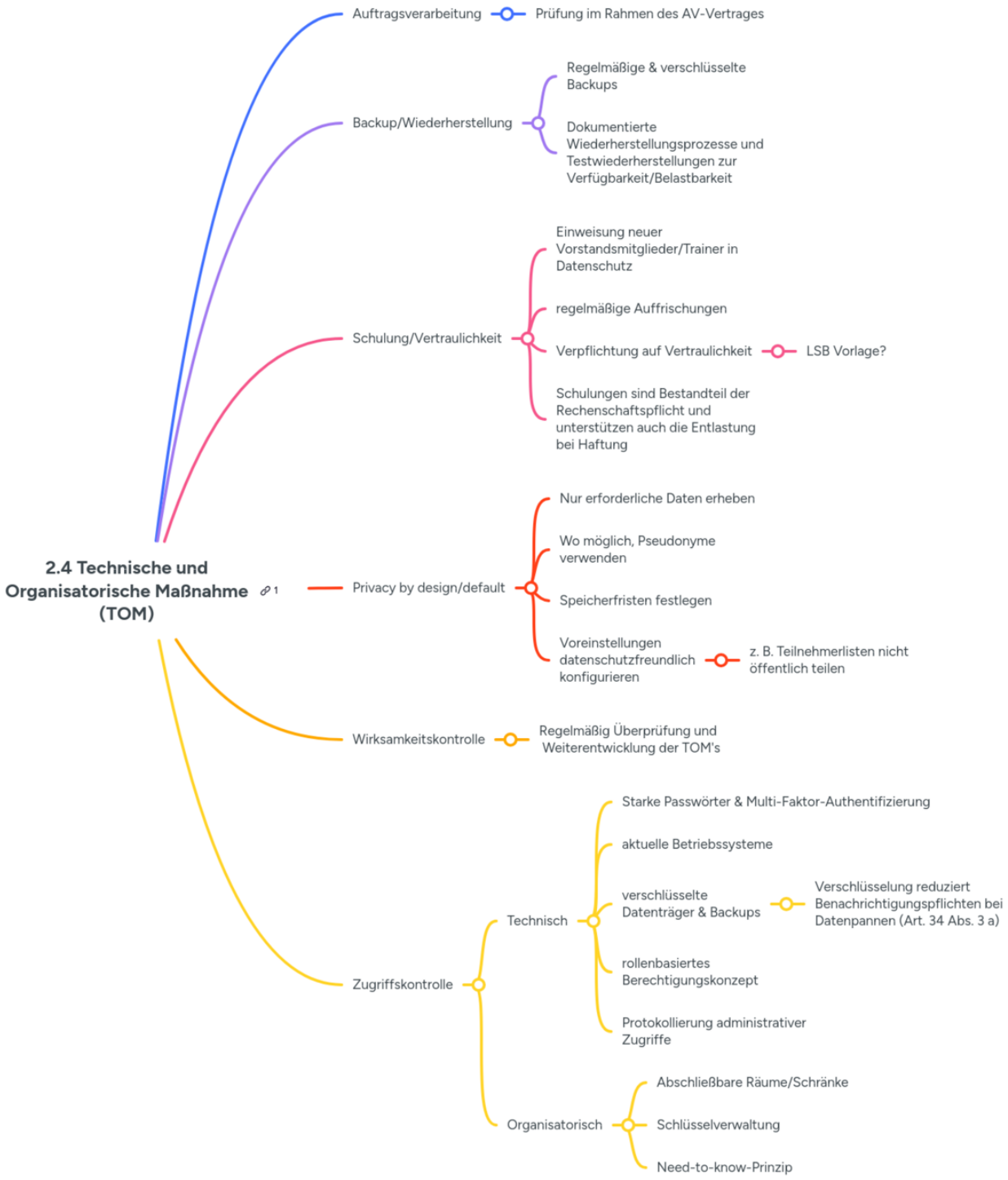
Beispiel

Beispiel

Die Mitgliederliste wird auf einem 12-stellig passwortgeschützten Computer (Passwortschutz = technische Maßnahme) gespeichert, auf den nur der geschäftsführende Vorstand durch einen Schlüssel zu einem feuerfesten Stahlschrank (Stahlschrank = organisatorische Maßnahme) Zugriff hat. Backups erfolgen verschlüsselt mind. wöchentlich, um ungewollten Datenverlust zu verhindern (Backups = technische Maßnahme). Papierlisten von Rehasport-Teilnehmenden werden darüber hinaus nur in einem abschließbaren feuerfesten Stahlschrank aufbewahrt, dessen Zugang nur den Rehasport-Trainern möglich ist (Beschränkung = organisatorische Maßnahme). Neue Vorstandsmitglieder erhalten eine Datenschutzschulung und werden auf Vertraulichkeit verpflichtet (Schulung = organisatorische Maßnahme).

Eine Auflistung weiterer Beispiele findet ihr in der MindMap.

MERKE: Eine nachvollziehbare Dokumentation und klare Prozesse sind die Basis, um im Fall von Anfragen oder Prüfungen durch die Aufsichtsbehörde schnell und sicher reagieren zu können. Es empfiehlt sich, auch ohne einen Datenschutzbeauftragten einen **Verantwortlichen für den Datenschutz** im Verein zu benennen.


2.4 Technische und Organisatorische Maßnahme (TOM)
1
Auftragsverarbeitung
Prüfung im Rahmen des AV-Vertrages
Backup/Wiederherstellung
Regelmäßige & verschlüsselte Backups
Dokumentierte Wiederherstellungsprozesse und Testwiederherstellungen zur Verfügbarkeit/Belastbarkeit
Schulung/Vertraulichkeit
Einweisung neuer Vorstandsmitglieder/Trainer in Datenschutz
regelmäßige Auffrischungen
Verpflichtung auf Vertraulichkeit
LSB Vorlage?
Schulungen sind Bestandteil der Rechenschaftspflicht und unterstützen auch die Entlastung bei Haftung
Privacy by design/default
Nur erforderliche Daten erheben
Wo möglich, Pseudonyme verwenden
Speicherfristen festlegen
Voreinstellungen datenschutzfreundlich konfigurieren
z. B. Teilnehmerlisten nicht öffentlich teilen
Wirksamkeitskontrolle
Regelmäßig Überprüfung und Weiterentwicklung der TOM's
Zugriffskontrolle
Technisch
Starke Passwörter & Multi-Faktor-Authentifizierung
aktuelle Betriebssysteme
verschlüsselte Datenträger & Backups
Verschlüsselung reduziert Benachrichtigungspflichten bei Datenpannen (Art. 34 Abs. 3 a)
rollenbasiertes Berechtigungskonzept
Protokollierung administrativer Zugriffe
Organisatorisch
Abschließbare Räume/Schränke
Schlüsselverwaltung
Need-to-know-Prinzip

Details

Autor:
Sandro Geil

zuletzt aktualisiert:
Februar 2026

Quelle:
Art. 6 Abs. 1 DSGVO

Art. 5 Abs. 2 DSGVO

Art. 15 DSGVO

Art. 24 DSGVO