**Unsere 10-Punkte-Liste für Vereine**

Letztendlich lassen sich die grundlegenden Pflichten in wenigen Punkten zusammenfassen.

1. Prüfen Sie, ob Sie einen Datenschutzbeauftragten benennen müssen. Das ist dann der Fall, wenn zehn oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Einige Beispiele, wann eine solche Verarbeitung im Verein vorliegt, finden Sie in der [Broschüre](https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/20180613_Datenschutz%20im%20Verein_3.pdf) des Hessischen Beauftragten für Datenschutz und Informationsfreiheit auf den Seiten 3 und 4.
2. Erstellen Sie ein [Verzeichnis der Verarbeitungstätigkeiten](https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf) gemäß Art. 30 DSGVO.
3. Prüfen Sie, ob Sie für alle Verarbeitungen eine Rechtsgrundlage haben. Bei Vereinen ist das in der Regel der Vertrag über die Mitgliedschaft in Verbindung mit der Vereinssatzung oder eine Einwilligung. Beispiele dazu, wann welche Rechtsgrundlage im Verein zum Tragen kommt, finden Sie in der [Broschüre](https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/20180613_Datenschutz%20im%20Verein_3.pdf) des Hessischen Beauftragten für Datenschutz und Informationsfreiheit auf den Seiten 1 und 2. Ein Muster für eine [Einwilligungserklärung für die Veröffentlichung von Mitgliederdaten im Internet](https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/03/Verein-Einwilligungserkl%C3%A4rung-angepasst.pdf) bietet der Landesbeauftragte für den Datenschutz Baden-Württemberg.
4. Informieren Sie Ihre Mitglieder über die Datenverarbeitungsvorgänge. Am einfachsten geschieht dies im Rahmen der Prozedur der Aufnahme als Mitglied, indem Sie zu dem Zeitpunkt ein Hinweisblatt austeilen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg bietet ein Muster bzw. eine Anleitung für die Informationspflicht bei Erhebung von personenbezogenen Daten ab Seite 12 seines [Praxisratgebers](https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf).
5. Achten Sie darauf, nur die personenbezogenen Daten zu verarbeiten, die für den Zweck erforderlich sind und löschen Sie die Daten, wenn diese nicht mehr erforderlich sind und keine gesetzlichen Aufbewahrungspflichten mehr bestehen.
6. Schließen Sie notwendige Auftragsverarbeitungsverträge mit Drittdienstleistern (beispielsweise bei Mitgliederverwaltung unter Nutzung einer Cloud-Lösung, Hosting).
7. Informieren und verpflichten Sie Personen, die mit personenbezogenen Daten umgehen, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DSGVO erfolgt. Hierfür bietet das BayLDA ein [Muster](https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf) an.
8. Stellen Sie sicher, dass Sie Ihre Pflichten, beispielsweise im Fall von Auskunftsersuchen durch betroffene Personen oder Löschungsverlangen, zeitnah nachkommen können. Bei Datenschutzverletzungen ist dies der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden ab Kenntnis zu melden.
9. Eine Datenschutz-Folgenabschätzung werden Sie in der Regel nicht durchführen müssen. Prüfen Sie dennoch, ob ein hohes Risiko bei der Datenverarbeitung im Verein besteht, in dem Fall müsste eine Datenschutz-Folgenabschätzung durchgeführt werden.
10. Achten Sie darauf, dass eine ausreichende Sicherheit bei der Verarbeitung personenbezogener Daten gegeben ist. Achten Sie insbesondere darauf, aktuelle Betriebssysteme und Anwendungen zu verwenden, kümmern Sie sich um den Passwortschutz, regelmäßige Backups, Virenscanner und schränken Sie Benutzerrechte so weit ein, dass nur Personen, die mit den Daten auch tatsächlich umgehen müssen, Zugang zu den jeweiligen personenbezogenen Daten haben.