

Datenschutzplan: Nachweis der DSGVO-Umsetzung im Verein

	ja	nein	Handlungsbedarf	Maßnahme	Erledigen bis	Erledigt
Dokumentation						
Haben Sie eine Liste mit den Prozessen in Ihrem Verein?						
Ist für jeden Prozess ein Verzeichnisse vorhanden?						
Zugang und Arbeitsplätze						
Eingang: Gibt es eine Zutrittskontrolle (Schlüssel, ...)?						
Sind Bildschirme, Fax und andere Geräte vor dem Einblick Dritter geschützt?						
Ist festgelegt, wer auf welche Daten zugreifen kann?						
Passwortschutz und -wechsel						
Ist gesichert, dass nur Berechtigte auf Daten zugreifen können (Passwortschutz)?						
Werden die Passwörter regelmäßig ausgetauscht?						
Wird dieser Austausch kontrolliert?						
Werden Nutzerwechsel und Zugriffsmöglichkeiten der Mitarbeiter beim Passwortwechsel berücksichtigt?						
Datensicherheit						
Sichern Sie Daten regelmäßig (auf Smartphone und Tablet genauso wie auf stationären PC)?						
Sind die vorhandenen Datenverarbeitungssysteme bekannt?						
Sind die Datenverarbeitungssysteme physisch geschützt (z. B. abschließbarer Serverraum)?						
Gibt es Virenschutzprogramme?						
Ist eine Absicherung gegen Diebstahl und Einbruch vorhanden bzw. vorgesehen?						
Sind Ihre Mitarbeiter auf das Datengeheimnis auch nach der neuen DSGVO verpflichtet?						
Haben Sie Ihre Mitarbeiter im Umgang mit Daten und dem Datenschutz geschult? Können Einhaltung sicherstellen?						
Löschen Sie nicht mehr benötigte Daten regelmäßig innerhalb der Löschfristen?						

	ja	nein	Handlungsbedarf	Maßnahme	Erledigen bis	Erledigt
Rechte der Beschäftigten/Mitarbeiter						
Haben Sie eine schriftliche Einwilligung der Mitarbeiter in die Verarbeitung personenbezogener Daten?						
Haben Sie den Mitarbeiter über den Zweck der Datenverarbeitung und über sein Widerrufsrecht nach Art. 7 Abs. 2 und 3 DSGVO aufgeklärt?						
Sind Arbeitsvertrag und die Einwilligung in Datenverarbeitungen zwei getrennte Dokumente?						
Verarbeiten Sie auf der Grundlage einer Einwilligung auch besondere Kategorien personenbezogener Daten? Haben Sie im Rahmen einer Einwilligung hierauf gesondert hingewiesen?						
Bewerbungsverfahren						
Laufen Bewerbungen einheitlich über ein verschlüsseltes E-Mail-Postfach ein, z. B. bewerbung@verein.de?						
Halten Sie den Bewerberdatenschutz ein? Haben Sie alle erforderlichen Maßnahmen getroffen, um den Schutz der personenbezogenen Daten einheitlich und lückenlos zu gewährleisten? Dokumentieren Sie diesen Prozess?						
Informieren Sie den Bewerber bei Eingang der Unterlagen über die Art der Datenerhebung (zum Verarbeitungszweck sowie zur Dauer des Aufbewahrungszeitraums) – z. B. mithilfe einer automatischen Eingangsbestätigung?						
Nach beendetem Bewerbungsverfahren sind Unterlagen/Daten der abgelehnten Bewerber zurückzuschicken, zu löschen oder zu vernichten. Halten Sie sich an die Fristen (Unterlagen/Daten dürfen mindestens 4 Monate, aber maximal 6 Monate vorgehalten werden; länger darf nur mit Zustimmung der jeweiligen Person gespeichert werden)?						
Rechte der Mitglieder						
Ist durch Verfahren sichergestellt, dass die Mitglieder ihr • Informationsrecht, • Auskunftsrecht, • Berichtigungsrecht und • Widerspruchsrecht ausüben können?						
Haben Sie für die Datenerhebung, Speicherung und Verarbeitung eine DSGVO-wirksame Einwilligung?						
Haben Sie Vordrucke für künftige Einwilligungen ab Inkrafttreten der DSGVO vorbereitet?						
Haben Sie einen Datenschutzbeauftragten bestellt, weil im Verein mehr als 9 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind?						
Haben Sie alle Auftragsverarbeiter in einem Verarbeitungsverzeichnis erfasst?						
Haben Sie datenschutzkonforme Verträge mit den Auftragsverarbeitern geschlossen?						
Haben Sie sich von Ihren Auftragsverarbeitern deren TOM zeigen lassen, mit denen sie Datenschutz und Datensicherheit der ihnen überlassenen Daten gewährleisten?						

	ja	nein	Handlungsbedarf	Maßnahme	Erledigen bis	Erledigt
Haben Sie für eine den Löschfristen angepasste Vorgehensweise gesorgt („Löschroutine“), d. h. • vorhandene Daten ermittelt? • Daten, die definitiv nicht mehr benötigt werden, gekennzeichnet? • die Aufbewahrungspflicht der jeweiligen Daten geprüft?						
Können Sie Verstöße gegen den Datenschutz feststellen bzw. verhindern?						
Haben Sie ggf. ein Muster für das Meldeverfahren bei Datenschutzverstößen vorbereitet, um einen Verstoß bei der zuständigen Meldebehörde innerhalb von 72 Stunden melden zu können?						
Datenvernichtung						
Haben Sie ein Konzept (Schutzklassen, Sicherheitsstufen, Datenträger und Vernichtungsmaßnahmen), das den Schutzbedarf Ihrer personenbezogenen Daten festlegt?						
Haben Sie die Daten-Vernichtungsmaßnahmen in Ihrem Verein an Schutzklassen und Sicherheitsstufen angepasst, z. B. dass zur Vernichtung von Personaldaten Ihr Aktenvernichter die Sicherheitsstufe 4 besitzt?						
Haben Sie Verantwortliche für die Datenvernichtung festgelegt?						
Haben Sie Ihre Mitarbeiter geschult und Sie auch auf besondere datenschutzrelevante Gefahren in Ihrem Verein aufmerksam gemacht, z. B. dass vergessene Dokumente aus dem Fax/Kopierer nicht neben das Gerät gelegt werden dürfen?						
Haben Sie Regeln für den Umgang mit der Datenvernichtung bestimmt?						
Haben Sie festgelegt, wann im Jahr die Daten in Papierform in Ihrem Verein durchgesehen und geordnet werden (welche bleiben, welche werden vernichtet oder in ein sicheres, externes Archiv verlagert)?						
Haben Sie dafür gesorgt, dass die Vernichtung rechtmäßig erfolgt und dafür TOM in Ihrem Verein umgesetzt?						

Wichtiger Hinweis:

Der Inhalt ist nach bestem Wissen und Kenntnisstand erstellt worden. Die Redaktion prüft ihn regelmäßig und passt ihn gegebenenfalls an. Gleichwohl schließen wir Haftung und Gewähr aus, da die Materie komplex ist und sich ständig wandelt. Muster dienen als Vorlage und sind individuell anzupassen.