Checkliste zum neuen Datenschutzgesetz

Die nachfolgende Checkliste bietet einen Überblick über die wichtigsten Massnahmen, die Vereine im Hinblick auf das Inkrafttreten des neuen Datenschutzgesetzes am 1. September 2023 treffen sollten. Dabei wird zwischen den Kategorien «Must have» (gesetzlich vorgeschrieben) und «Nice to have» (empfohlen) unterschieden.

	Must have	Nice to have
Datenschutzstrategie		Es wird die Erstellung eines **Planes zur Erreichung der Compliance** (Erstellung notwendiger Dokumente und Prozesse etc.) bis zum 1. September 2023 empfohlen, inkl. Verantwortlichkeiten, Ziele und Terminplan.
Verzeichnis der Bearbeitungstätigkeiten	Verantwortliche müssen ein Verzeichnis aller ihrer Datenbearbeitungen erstellen und dieses regelmässig nachführen, sofern sie mindestens **250 Mitarbeitende** beschäftigen. Die Pflicht besteht unabhängig von der Mitarbeiterzahl, wenn sie **umfangreich besonders schützenswerte Personendaten** bearbeiten oder **Profiling mit hohem Risiko** vornehmen.	Auch in Fällen, in denen die Erstellung eines Verzeichnisses nicht zwingend ist, wird ein derartiges **Inventar der Datenbearbeitungen** empfohlen, da in jedem Datenschutz-Compliance-Projekt als erster Schritt festgestellt werden sollte, welche Daten wie und wozu bearbeitet werden.
Datenschutz-Risikomanagement	Eine **Datenschutz-Folgenabschätzung** ist vorzunehmen, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Dies erfordert **Prozesse zur Bewertung des Risikos** und zur **Durchführung einer Datenschutz-Folgenabschätzung**.	

	Must have	Nice to have
Informationspflicht gegenüber betroffenen Personen	Bei der Beschaffung von Personendaten ist die betroffene Person **über die geplante Datenbearbeitung zu informieren**. Dabei sind ihr diejenigen Informationen mitzuteilen, die erforderlich sind, damit sie Ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleisten.	Die Information hat nicht zwingend schriftlich zu erfolgen. Dies wird jedoch aus beweisrechtlichen und praktischen Gründen sehr empfohlen. Die Informationspflicht wird in der Regel durch **Datenschutzerklärungen** erfüllt, z.B. im Rahmen der Registrierung als Vereinsmitglied, auf der Website, gegenüber Mitarbeitenden.
Interne Reglemente/Richtlinien	Unter gewissen Umständen besteht die Pflicht zur Führung eines **Protokolls** der Datenbearbeitungen und zur Erstellung eines **Bearbeitungsreglements**, namentlich wenn besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird.	Unabhängig von diesen allfälligen Pflichten wird zum Zweck der Sicherstellung der Einhaltung der Datenschutzregeln die Erstellung **einer internen Richtlinie** empfohlen mit **Anweisungen** an Vereinsfunktionäre und Mitarbeitende, wie diese mit Personendaten und mit der Informationssicherheit umzugehen haben. Darin können auch interne **Verantwortlichkeiten und Rollen** bezüglich Datenschutz festgelegt werden.
Datenbearbeitung durch Dritte	Bei **Auslagerung von Datenbearbeitungen an Dritte** (z.B. an eine IT-Firma, welche die Website des Vereins hostet und dabei Zugriff auf Personendaten hat) ist sicherzustellen, dass diese die **Personendaten nur so bearbeiten, wie es der Verantwortliche selbst tun dürfte** und dass die Dritten die **Datensicherheit** gewährleisten können.	Aus beweisrechtlichen und praktischen Gründen empfiehlt sich, mit den Dritten einen **schriftlichen Auftragsbearbeitungsvertrag** abzuschliessen und darin die Rechte und Pflichten zwischen Verantwortlichem und Auftragsbearbeiter zu definieren.

	Must have	Nice to have
Regelung zu Aufbewahrungs- und Löschpflichten	Der Grundsatz der **Zweckgebundenheit** besagt, dass Personendaten nur zu dem Zweck bearbeitet werden, der bei ihrer Beschaffung angegeben wurde, gesetzlich vorgeschrieben ist oder sich aus den Umständen ergibt. Folglich sind **Daten nach Erreichung des Zwecks** (z.B. Ausscheiden eines Vereinsmitglieds) **grundsätzlich zu löschen**, vorbehaltlich zwingender längerer **Aufbewahrungspflichten** (z.B. 10 Jahre für Buchhaltungsbelege) oder anderweitiger Rechtfertigungsgründe.	Es wird die Erstellung einer **internen Regelung** hinsichtlich der Pflichten im Zusammenhang mit der Aufbewahrung und Löschung von Personendaten empfohlen. Diese kann auch in die oben erwähnte interne Richtlinie integriert werden.
Datensicherheit	Verantwortliche haben eine dem Risiko angemessene Datensicherheit durch geeignete **technische und organisatorische Massnahmen** (TOM) zu gewährleisten.	Es wird empfohlen, die **TOM schriftlich** festzuhalten.
	Bei einem **Datensicherheitsvorfall** (bspw. wenn Personendaten unbeabsichtigt Unbefugten offengelegt oder zugänglich gemacht werden) ist bei einem hohen Risiko der EDÖB so rasch als möglich zu informieren. Die betroffene Person ist ebenfalls zu informieren, sofern dies zu deren Schutz notwendig ist.	Es empfiehlt sich ggf., einen **schriftlichen Prozess** zur Beurteilung des Risikos eines Datensicherheitsvorfalls und zur allfälligen Meldung an den EDÖB und an die betroffene Person zu erstellen, inkl. Handlungsanweisungen und Verantwortlichkeiten.

	Must have	Nice to have
Betroffenenrechte	**Auskunftsrecht**: Die betroffene Person kann Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Der Verein muss in der Lage sein, entsprechend Auskunft zu geben.	Gegebenenfalls empfiehlt sich die Einführung eines **schriftlichen Prozesses** zur Handhabung von entsprechenden Anfragen und Begehren, inkl. Handlungsanweisungen und Verantwortlichkeiten. Im Rahmen des Grundsatzes der Richtigkeit wird ausserdem empfohlen, einen Prozess zur **regelmässigen Prüfung** der vom Verein bearbeiteten Personendaten einzuführen.
	Berichtigungsrecht: Die betroffene Person kann verlangen, dass unrichtige Personendaten berichtigt werden. Der Verein muss in der Lage sein, Daten zu korrigieren.	
	Datenportabilität: Die betroffene Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten verlangen, die sie ihm bekanntgegeben hat und die dieser automatisiert bearbeitet hat. Der Verein muss in der Lage sein, der betroffenen Person ihre Daten in einem gängigen elektronischen Format herauszugeben oder auf Wunsch einem anderen Verantwortlichen zu übertragen.	
Datenübermittlungen ins Ausland	Werden **Daten ins Ausland übermittelt**, hat der Verantwortliche den Datenschutz sicherzustellen, einschliesslich wenn ein Datenbearbeiter **aus dem Ausland Zugriff auf Personendaten** des Vereins hat. Namentlich sind bei einer Datenübermittlung in ein Empfängerland ohne **adäquates Datenschutzniveau** (z.B. USA) zusätzliche **Garantien** vorzusehen (z.B. Standarddatenschutzklauseln) und vor der Übermittlung eine **Datentransfer-Folgenabschätzung** durchzuführen.	Es wird empfohlen, den Prozess zur Beurteilung des Empfängerlands und zur Einführung von ggf. notwendigen zusätzlichen Garantien und Massnahmen **schriftlich** festzuhalten, inkl. Handlungsanweisungen und Verantwortlichkeiten.

	Must have	Nice to have
Datenschutzbewusstsein / Schulungen		Die Umsetzung und Einhaltung der datenschutzrechtlichen Bestimmungen und der internen Richtlinien erfordert ein entsprechendes Bewusstsein innerhalb des Vereins. Entsprechend wird die Durchführung von regelmässigen **Datenschutz-Schulungen** empfohlen.
Datenschutzberater		Die Ernennung eines (internen oder externen) **Datenschutzberaters**, dessen Kontaktdaten beim EDÖB zu melden sind, ist nicht zwingend, kann gegebenenfalls aber sinnvoll sein.
Regelmässige Überprüfung der datenschutzrechtlichen Massnahmen		Es wird empfohlen, die datenschutzrechtlichen Massnahmen und deren **Einhaltung regelmässig zu prüfen und zu aktualisieren**.