



Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.

Hinweis:

Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. Verantwortlicher. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält. In der folgenden Übersicht werden die wesentlichen Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

Kurzbeschreibung des Vereins

Ein kleiner Sportverein hat 200 Mitglieder, einen ersten Vorstand, einen Kassier sowie einen Schriftführer (Vorstand im Sinne des BGB) sowie fünf Personen, die nach der sog. Übungsleiterpauschale bezahlt werden. Die Mitgliederverwaltung erfolgt durch den Schriftführer selbst. Die Verwaltung der Mitgliedsbeiträge erfolgt dagegen durch den Kassier. Der Verein betreibt zudem eine kleine Webseite, die bei einem Dienstleister gehostet ist, mit Mitgliederfotos.

Wesentliche Verarbeitungstätigkeiten **sind z. B.:**

- Lohnabrechnung (über einen externen Dienstleister)
- Mitgliederverwaltung
- Betrieb der Webseite des Sportvereins (über Hosting-Paket eines externen Dienstleisters)
- Veröffentlichung von Mitgliederfotos auf der eigenen Webseite
- Beitragsverwaltung

Wesentliche DS-GVO-Anforderungen für den Verein

A Datenschutzbeauftragter (DSB)

Muss ein DSB vom Verein benannt werden?

- ja
 nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten

Ist ein *solches* Verzeichnis erforderlich?

- ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
 nein

C Datenschutz-Verpflichtung von Beschäftigten

Ist eine *solche* Verpflichtung durchzuführen?

- ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
 nein

D Information- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

- ja (insb. in der Vereinssatzung sowie auf der Webseite in der Datenschutzerklärung)
 nein

E Löschen von Daten

Gibt es eine *Anforderung* zur Datenlöschung?

- ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
 nein

F Sicherheit

Müssen die Daten besonders gesichert werden?

- ja
 nein (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)

G Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

- ja (sowohl mit dem Hosting-Anbieter als auch mit dem externen Lohnabrechner)
 nein

H Datenschutzverletzungen

Müssen bestimmte *Vorfälle gemeldet werden*?

- ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
 nein

I Datenschutz-Folgeabschätzung (DSFA)

Muss eine DSFA vom Verein durchgeführt werden?

- ja
 nein (da kein hohes Risiko bei der Datenverarbeitung im Verein besteht)

J Videoüberwachung (VÜ)

Besteht eine Ausschuldungspflicht bezüglich VÜ?

- ja
 nein (da keine Videoüberwachung im Verein durchgeführt wird)



i Erläuterungen zu den Anforderungen

A Datenschutzbeauftragter (DSB)

In aller Regel ist nur dann ein DSB zu benennen, wenn mindestens 10 *Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. „Ständig beschäftigt“ ist, wer z. B. permanent Mitgliederverwaltung macht - „nicht ständig beschäftigt“ ist dagegen bspw., wer als Übungsleiter nur mit den Namen seiner Mannschaft umgeht.

⇒ DSK-Kurzpapier Nr. 12: www.lida.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf

B Verzeichnis von Verarbeitungstätigkeiten

Vereine, die regelmäßige Mitgliederverwaltung und Beitragsabrechnung machen, müssen ein – vom Umfang her sehr überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.

⇒ BayLDA Muster-Verzeichnis für kleine Vereine: www.lida.bayern.de/media/muster_1_verein_verzeichnis.pdf

⇒ DSK-Kurzpapier Nr. 1: www.lida.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf

⇒ DSK-Muster-Verzeichnis allgemein: www.lida.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf

C Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.

⇒ BayLDA Info-Blatt zur Verpflichtung: www.lida.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

D Informations- und Auskunftspflichten

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Ein Verein muss bspw. Informationen auf der Homepage und der Satzung leicht zugänglich bereithalten. Die betroffenen Personen (z. B. Vereinsmitglieder) haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.

⇒ DSK-Kurzpapier Nr. 6: www.lida.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf

⇒ DSK-Kurzpapier Nr. 10: www.lida.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

E Löschen von Daten

Sobald keine gesetzliche Grundlage (z. B. steuerliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. In der Regel ist dies bspw. erst der Fall nach Ausscheiden eines Vereinsmitglieds.

⇒ DSK-Kurzpapier Nr. 11: www.lida.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf

F Sicherheit

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virens Scanner und Benutzerrechte. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können.

⇒ BayLDA-Kurzpapier Nr. 1: www.lida.bayern.de/media/baylda_ds-gvo_1_security.pdf

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. Buchhaltung) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.

⇒ DSK-Kurzpapier Nr. 13: www.lida.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

⇒ BayLDA-Formulierungshilfe zum Vertrag: www.lida.bayern.de/media/muster_adv.pdf

H Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Vereinsdaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

⇒ BayLDA-Kurzpapier Nr. 8: www.lida.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

⇒ BayLDA-Online-Service zur Meldung: www.lida.bayern.de/de/datenpanne.html

I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgeabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

⇒ DSK-Kurzpapier Nr. 5: www.lida.bayern.de/media/dsk_kpnr_5_dsfa.pdf

J Videoüberwachung

Führt ein Verantwortlicher eine Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoaufnahmen zu informieren.

⇒ DSK-Kurzpapier Nr. 15: www.lida.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf