



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

Muster 4: Steuerberater

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 **Steuerberaters**

Ein Steuerberater betreibt mit einem angestellten Steuerberater eine Steuerberaterkanzlei. Beide werden von vier Steuerfachangestellten, einem Bilanzbuchhalter und einer Telefonkraft unterstützt. Dabei werden Privat- und Firmenkunden betreut. Die Kanzlei hat ein Softwarehaus, das die Webseite hostet und die IT wartet.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohn- und Gehaltsabrechnung der Mitarbeiter
- Verarbeitung von Mandantendaten von Privatkunden zur Beratung und Rechnungsstellung
- Verarbeitung von Mandantendaten von Firmenkunden und deren Kunden/Mitarbeitern zur Beratung und Rechnungsstellung
- Betrieb der Webseite über Dienstleister

☑️ **Wesentliche DS-GVO-Anforderungen für den Steuerberater**

A **Datenschutzbeauftragter (DSB)**

Muss ein DSB vom Steuerberater 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. bei Vertragsabschluss 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 (neben Standardmaßnahmen muss u. a. beim Transport auf Verschlüsselung geachtet werden)
 nein

G **Auftragsverarbeitung**

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

- ja (bzgl. dem IT-Dienstleister für Webseite und Wartung der Kanzlei-IT)
 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)**

Ist eine DSFA vom Steuerberater durchzuführen?

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

J **Videoüberwachung (VÜ)**

Besteht eine Ausschilderungspflicht bezüglich VÜ?

- ja
 nein (da keine Videoüberwachung vom Steuerberater durchgeführt wird)



① 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 Mandantenbetreuung macht. „Nicht ständig beschäftigt“ ist dagegen bspw., wer als Putzkraft nur die Möglichkeit hat, Daten einzusehen.

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

B Verzeichnis von Verarbeitungstätigkeiten

Steuerberater müssen ein Verzeichnis ihrer Verarbeitungstätigkeiten führen.

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

⇒ DSK-Muster-Verzeichnis allgemein: www.lda.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.

⇒ DSK-Kurzpapier Nr. 19: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

D Informations- und Auskunftspflichten

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich sind (z.B. Vertragsanlage, Homepage). Die betroffenen Personen haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten

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

⇒ DSK-Kurzpapier Nr. 10: www.lda.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.

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

F Sicherheit

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind viele Standardmaßnahmen hilfreich. Dazu gehören u. a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virens Scanner und Benutzerrechte. Bei der Kommunikation mit Mandanten ist jedoch darauf zu achten, dass eine ausreichende Verschlüsselung eingesetzt wird.

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

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. IT Wartung oder Webhosting) 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.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

⇒ BayLDA-Formulierungshilfe zum Vertrag: www.lda.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 Mandantendaten), 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.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

⇒ BayLDA-Online-Service zur Meldung: www.lda.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.lda.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.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf