Bayerisches Landesamt für
Datenschutzaufsicht

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

Muster 2: Kfz-Werkstatt

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 der Kfz-Werkstatt

Die Kfz-Werkstatt hat 20 Beschäftigte. Neben den Mitarbeiterdaten verarbeitet sie hauptsächlich Kunden- und Fahrzeugdaten, die im Rahmen von Kfz-Dienstleistungen anfallen (z .B. Kundendienst, TÜV-Untersuchung, Reparaturen). Bei Reparaturaufträgen lesen die Mechatroniker über die OBD-Schnittstelle den Fehlerspeicher der Fahrzeuge aus. Buchhaltung und Lohnabrechnung für die eigenen Mitarbeiter macht ein Steuerberater.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung (über einen Steuerberater)
- Personalverwaltung
- Betrieb der Firmenwebseite (über Hosting-Paket eines Dienstleisters)
- Digitale Auftragsverwaltung inkl. Kundenstamm und Fahrzeugdaten
- IT-Support (über externen Dienstleister)
- Auswerten von Fahrzeugdaten

Wesentliche DS-GVO-Anforderungen für die Kfz-Werkstatt

A Datenschutzbeauftragter (DSB)
Muss die Kfz-Werkstatt einen DSB benennen?
☐ 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. zu Kundendaten 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 (mit dem Hosting-Anbieter sowie dem IT-Support-Dienstleister)
☐ 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 die Kfz-Werkstatt eine DSFA durchführen?
☐ ja
☒ nein (da kein hohes Risiko bei der Datenverarbeitung besteht)

J Videoüberwachung
Besteht eine Ausschilderungspflicht bezüglich VÜ?
☐ ja
☒ nein (da keine Videoüberwachung durchgeführt wird)

ⓘ 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 Kunden- oder Personalverwaltung macht. Dazu zählen nicht Mechatroniker, die lediglich bei der Bearbeitung von Reparaturaufträgen per OBD-Schnittstelle die Fehlerspeicher der Fahrzeuge auslesen.

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

B Verzeichnis von Verarbeitungstätigkeiten

Kfz-Werkstätten gehen regelmäßige mit Kunden- und Mitarbeiterdaten um und müssen ein – vom Umfang her überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.

⇨ **BayLDA Muster-Verzeichnis für Kfz-Werkstätten:** *www.lda.bayern.de/media/muster_2_kfz-werkstatt_verzeichnis.pdf*
⇨ **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 DSG-GVO erfolgt.

⇨ **BayLDA Info-Blatt zur Verpflichtung:** *www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf*

D Informations- und Auskunftspflichten

Jede Kfz-Werkstatt hat betroffene Personen (d. h. insbesondere Kunden und Mitarbeiter) schon bei der Datenerhebung über die Verarbeitung ihrer personenbezogenen Daten zu informieren. 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 oder handelsrechtliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. Dies ist z. B. der Fall, wenn ein Kunde mehrere Jahre lang keine neuen Aufträge mehr erteilt hat.

⇨ **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 Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u. a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virenscanner und Benutzerrechte.

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

G Auftragsverarbeitung

Sobald Kfz-Werkstätten externe Dienstleistungen (z.B. Hosting der Webseite, IT-Support) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, müssen sie mit dem Dienstleister einen schriftlichen Vertrag zur Auftragsverarbeitung abschließen.

⇨ **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, Verlust von Tablet oder Smartphone mit unverschlüsselten Kundendaten, Fehlversendung der Rechnung), 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-Folgenabschätzung 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 eine Kfz-Werkstatt Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich.

⇨ **DSK-Kurzpapier Nr. 15:** *www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf*

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 2: Kfz-Werkstatt – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
XYZ Schraub GmbH
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@xyzschraub.de
Web: www.xyzschraub.de

Geschäftsführer: Martin Eckfelder-Grün, geb. 03.02.1972

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohn-abrechnung (über Steuerberater)	Herbert Bauer 0981/123456-1 herbert@ xyzschraub.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name, Geburtsdatum • Adresse • Bankverbindungsdaten • Lohn-/Entgeltdaten ...	Steuer-berater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Personal-verwaltung	Herbert Bauer 0981/123456-1 herbert@ xyzschraub.de	02.03.2018	• Personaladministration • Personalführung • Arbeitszeitverwaltung • Personalbeschaffung (betrifft Bewerber)	• Beschäftigte • Bewerber	• Name, Adressen • Zeitwirtschaftsdaten • Daten zur Arbeitsleistung • Leistungsbeurteilung • Lebenslauf und Bewerbungsunterlagen (betr. Bewerber) ...	Keine	Keine	• Beschäftigte: in der Regel ca. 3 Jahre nach Ausscheiden • abgelehnte Bewerber: 6 Monate nach Abschluss des Bewerbungs-verfahrens	Siehe IT-Sicherheits-konzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Max Meier 0981/123456-3 max@xyzschraub.de	28.02.2018	Außendarstellung	Webseitennutzer	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheits-konzept + HTTPS-Verschlüsselung
Auftrags-verwaltung inkl. Kundenstamm	Thomas Kleinlein 0981/123456-2 tom@xyzschraub.de	02.03.2018	• Bearbeitung von Aufträgen und Bestellungen inkl. Rechnungstellung • postalische Werbung	Kunden	• Name, Adresse • Angaben zum Auftrag • ggf. Bankverbindungsdaten • Fahrzeugdaten	Kfz-Hersteller	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
IT-Support (extern)	Max Meier (Tel. -3) max@xyzschraub.de	02.03.2018	Wiederherstellen eines laufenden IT-Betriebs (Verfügbarkeit) nach Bedarf	Beschäftigte Kunden Webseitennutzer	• Name • Nutzerkennung ...	Support-Dienstleister	Keine	...	Siehe IT-Sicherheits-konzept
Auswerten von Fahrzeugdaten	Rudi Piste (Tel. -4) rudi@xyzschraub.de	02.03.2018	Fehleranalyse / Reparatur	Kunden	• Fahrzeug-ID ...	Keine	Keine	...	...
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder