



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

Muster 3: Handwerksbetrieb

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 **Handwerksbetriebs**

Der Handwerksbetrieb (Installationsfirma) hat 50 Beschäftigte (eine Chefin, drei Beschäftigte in der Personalverwaltung, sieben in der Kundenverwaltung, drei Meister, zehn Gesellen, vier Azubis und 22 sonstige Mitarbeiter für Produktion und Handwerk). Buchhaltung und Steuerangelegenheiten macht ein Steuerberater. Die Firma betreibt selbst eine Webseite.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung (über einen Steuerberater)
- Personalverwaltung
- Betrieb der Firmenwebseite (über umfassendes Hosting-Paket eines externen Dienstleisters)
- Kundenverwaltung

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

A **Datenschutzbeauftragter (DSB)**

Muss ein DSB benannt werden?

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

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 (z. B. eigene Mitarbeiter, Kunden bei Auftragsannahme, Datenschutzerklärung der Webseite)
 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, der die Webseite bereitstellt und Services dazu anbietet)
 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 der Handwerksbetrieb eine DSFA durchführen?

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

J **Videoüberwachung (VÜ)**

Besteht eine Ausschilderungspflicht bezüglich VÜ?

- ja
 nein (da keine Videoüberwachung praktiziert 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 Kunden- oder Personalverwaltung macht. „Nicht“ dagegen, wer z. B. als Handwerker oder Produktionsmitarbeiter nur mit Namen und Adressen von Kunden umgeht.

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

B Verzeichnis von Verarbeitungstätigkeiten

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

⇒ BayLDA Muster-Verzeichnis für Handwerksbetriebe: www.lda.bayern.de/media/muster_3_handwerksbetrieb_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 DS-GVO erfolgt.

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

D Informations- und Auskunftspflichten

Jeder Handwerksbetrieb hat die betroffenen 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) für die Speicherung von personenbezogenen Daten mehr 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, Virens Scanner und Benutzerrechte.

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

G Auftragsverarbeitung

Sofern Handwerksbetriebe externe Dienstleistungen (z.B. Buchhaltung oder Hosting der Webseite) 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. Der Steuerberater gilt jedoch nicht als Auftragsverarbeiter, sondern als eigenständiger Verantwortlicher, mit diesem ist daher kein 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, 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-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 Handwerksbetrieb Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoüberwachung zu informieren.

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



Muster 3: Handwerksbetrieb – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

ABC Install GmbH
Steinbauerstr. 45a
98123 Sonsthausen

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

Geschäftsführerin: Susanne Kühnlein, geb. 03.12.1952

Verarbeitungstätigkeit	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@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern 	Beschäftigte	<ul style="list-style-type: none"> Name, Geburtsdatum Adresse Bankverbindungsdaten Lohn-/Entgeltdaten ggf. Religionszugehörigkeit Sozialversicherungsdaten Steuerdaten (Steuerklasse, Freibeträge,...) Berufsgenossenschaftsangaben 	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Personalverwaltung	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> Personaladministration Personalführung Arbeitszeitverwaltung Personalbeschaffung (betrifft Bewerber) 	<ul style="list-style-type: none"> Beschäftigte Auszubildende Bewerber 	<ul style="list-style-type: none"> Name, Adressen Zeitwirtschaftsdaten Daten zur Arbeitsleistung Leistungsbeurteilung Lebenslauf und Bewerbungsunterlagen (betr. Bewerber) 	Keine	Keine	<ul style="list-style-type: none"> Beschäftigte: in der Regel ca. 3 Jahre nach Ausscheiden abgelehnte Bewerber: 6 Monate nach Abschluss des Bewerbungsverfahrens 	Siehe IT-Sicherheitskonzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@abcinstall.de	28.02.2018	Außendarstellung	<ul style="list-style-type: none"> Webseitenbesucher 	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Kundenverwaltung	Janine Kleinlein 0981/123456-2 janine@abcinstall.de	02.03.2018	<ul style="list-style-type: none"> Bearbeitung von Aufträgen inkl. Rechnungstellung postalische Werbung 	Kunden	<ul style="list-style-type: none"> Name, Adresse Angaben zum Auftrag ggf. Bankverbindungsdaten 	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...

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 Virens Scanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder