Bayerisches Landesamt für
Datenschutzaufsicht

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

Muster 9: Online-Shop

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 Online-Shops

Ein kleines Startup-Unternehmen verkauft seine Produkte über eine eigene Webplattform, die auf Basis eines freien Content-Management-Systems bei einem Webhosting-Anbieter betrieben wird. Das Unternehmen hat neben dem Geschäftsführer noch vier Mitarbeiter, die in der Produktion tätig sind, sowie drei Mitarbeiter, die die Webplattform betreuen und sich schwerpunktmäßig um das Marketing kümmern.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung (über einen externen Dienstleister)
- Betrieb der Webseite des Startups (über Hosting-Paket eines externen Dienstleisters)
- Kundenverwaltung
- Zahlungsabwicklung bei Kunden (über einen externen Dienstleister)
- Werbemaßnahmen zur Kundengewinnung und -bindung

Wesentliche DS-GVO-Anforderungen für den Online-Shop

A Datenschutzbeauftragter (DSB)
Muss ein DSB vom Online-Shop 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 (bei den Mitarbeitern, die mit personenbezogenen Daten umgehen)
☐ nein

D Information- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
☒ ja (insb. auf der Webseite in der Datenschutzerklärung sowie bei Vertragsabschluss)
☐ nein

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
☒ ja (insb. der Kundendaten, aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
☒ ja (die auf der Webplattform verarbeiteten Daten müssen vor Angriffen geschützt werden)
☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
☒ ja (mit dem Hosting-Anbieter, dem Lohnabrechner und dem Zahlungsdienstleister)
☐ 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 Betrieb besteht)

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
☐ ja
☒ nein (da keine Videoüberwachung vom Unternehmen 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 Kundenverwaltung macht. „Nicht ständig beschäftigt" ist dagegen bspw., wer als Produktionsmitarbeiter ab und an mit den Kundennamen in Kontakt kommt.

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

B Verzeichnis von Verarbeitungstätigkeiten

Online-Shops, die regelmäßige Kundenverwaltung betreiben, müssen ein – vom Umfang her sehr überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.

⇨ **BayLDA Muster-Verzeichnis für kleine Online-Shops:** *www.lda.bayern.de/media/muster_9_online-shop_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 Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Online-Shops müssen insb. auf der Webseite Informationen zur Datenverarbeitung leicht zugänglich bereithalten. Die betroffenen Personen (z. B. Kunden) 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. Dies ist bspw. der Fall, wenn ein Kunde seit mehreren Jahren nichts mehr bestellt 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, muss neben den Standardmaßnahmen im Betrieb wie aktuelle Betriebssysteme, Passwortschutz, regelmäßige Backups, Virenscanner und Benutzerrechte die Webplattform ausreichend abgesichert werden. Insbesondere den realen Bedrohungen durch Cyberangriffen muss ausreichend Rechnung getragen werden.

⇨ **BayLDA-Kurzpapier Nr. 1:** *www.lda.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.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. Hacking des Online-Shops), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber innerhalb von 72 Stunden in Kenntnis zu setzen, betroffene Personen dagegen nur bei vorliegendem hohem Risiko (was eher selten der Fall ist).

⇨ **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 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*