Bayerisches Landesamt für
Datenschutzaufsicht

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

Muster 10: Bäckerei

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 Bäckerei

Der Bäckereibetrieb beschäftigt acht Personen (neben dem Inhaber drei angestellte Bäcker und fünf Verkäuferinnen). Mit der Datenverarbeitung für die Zwecke der Buchhaltung, von Steuerangelegenheiten und der kompletten Personalverwaltung einschließlich Lohnabrechnung ist ein Steuerberater beauftragt. Die Bäckerei hat zudem eine lediglich statische Webseite, auf der sie sich kurz vorstellt (Öffnungszeiten, Adresse, Produkte), ohne dass dort aber Bestellungen entgegengenommen werden.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung - komplett über Steuerberater (dieser ist selbst datenschutzrechtlich Verantwortlicher)
- Personalverwaltung - komplett über Steuerberater (dieser ist selbst datenschutzrechtlich Verantwortlicher)
- allenfalls gelegentlicher eigener Umgang mit personenbezogenen Daten von Mitarbeitern und Kunden

Wesentliche DS-GVO-Anforderungen für die Bäckerei

A Datenschutzbeauftragter (DSB)
Muss ein DSB von der Bäckerei benannt werden?
☐ ja
☒ nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten
Ist ein solches Verzeichnis erforderlich?
☐ ja
☒ nein (nur gelegentliche Verarbeitung personenbezogener Daten und kein hohes Risiko)

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
☒ ja (auch bei nur gelegentlichem Umgang mit personenbezogenen Daten z. B. von Kunden)
☐ nein

D Information- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
☒ ja (insbesondere bei der Erhebung von Mitarbeiterdaten, d. h. beim Abschluss des Arbeitsvertrags)
☐ 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
☒ nein (der Steuerberater und in diesem Fall auch der Web-Provider sind keine Auftragsverarbeiter)

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 Bäckerei 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 durch die Bäckerei stattfindet)

ⓘ 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 Bäcker oder Verkäufer nur gelegentlich 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

Die Bäckerei geht in diesem Beispielfall nur gelegentlich mit Kunden-/Mitarbeiterdaten um (z. B. bei einzelnen Bestellungen), da die Personalverwaltung inkl. Lohnabrechnung komplett auf einen Steuerberater ausgelagert ist. Dieser ist insoweit selbst datenschutzrechtlich Verantwortlicher – Personalverwaltung und Lohnabrechnung bleiben daher außen vor. Soweit die Bäckerei (gelegentlich) mit Kunden-/Mitarbeiterdaten umgeht, ist kein hohes Risiko für die Betroffenen erkennbar. Sie muss daher kein Verzeichnis von 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 auch nur gelegentlich mit personenbezogenen Daten z.B. von Kunden umgehen, zu informieren und dahingehend zu verpflichten, den Datenschutz zu beachten.

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

D Informations- und Auskunftspflichten

Der Betrieb hat die betroffenen Personen (etwa Kunden und Mitarbeiter) schon bei der Datenerhebung über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Mitarbeiter sind daher durch die Geschäftsleitung beim Eingehen des Arbeitsverhältnisses 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.

⇨ **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

Der Webhosting-Dienstleister ist nicht Auftragsverarbeiter, da es sich um eine rein statische Website handelt, auf der keine personenbezogene Daten im Auftrag der Bäckerei verarbeitet werden (soweit auf der Website IP-Adressen von Besuchern verarbeitet werden, handelt der Dienstleister als Telekommunikationsunternehmen, nicht als Auftragsverarbeiter).

⇨ **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 (wenn nur gelegentlichen) Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Verlust von Tablet oder Smartphone mit unverschlüsselten Kundendaten, Fehlversendung der Rechnung), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall 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 bei der Bäckerei jedoch nicht vorhanden.

⇨ **DSK-Kurzpapier Nr. 5:** *www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf*

J Videoüberwachung

Führt ein Betrieb Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich.

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