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

(Folgendes Musterbeispiel basiert auf einem entsprechend überarbeitetem Muster für Arztpraxen vom Bayerischen Landesamt für Datenschutzaufsicht)

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 DSGVO 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.

Musterbeispiel: Kleiner Taxibetrieb

Kurzbeschreibung des Taxiunternehmens

Das kleine Taxiunternehmen auf dem Land betreibt mit 7 Fahrern (einschließlich Unternehmer und Ehefrau) 3 Fahrzeuge bei eigener Vermittlung. Das Unternehmen betreibt eine kleine Webseite mit Hilfe eines Content Management Systems, auf dem online Fahrten gebucht werden können. Ein externer Dienstleister betreut die Webseite und die Unternehmens-IT. Die Datenverarbeitung der Krankenfahrten erfolgt auf eigenen Computern und einem Server innerhalb des Unternehmens.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohn- und Gehaltsabrechnung der Mitarbeiter
- Verarbeitung von Versichertendaten zur Abrechnung mit den Krankenkassen
- Betrieb der Webseite mit der Online-Terminbuchungsmöglichkeit

Wesentliche DS-GVO-Anforderungen für das Taxiunternehmen

A Datenschutzbeauftragter (DSB)
Muss ein DSB 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. durch Einwilligungserklärung zur Krankenfahrtenabrechnung sowie auf der Webseite in der Datenschutzerklärung)
- ☐ nein

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
- ☒ ja (aber erst nach Ablauf gesetzlicher Aufbewahrungs-pflichten)
- ☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
- ☒ ja (da sensible Daten verarbeitet werden, sind weitere Schutzmaßnahmen erforderlich)
- ☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
- ☒ ja (mit dem IT-Betreuer, der die Webseite und die Vermittlungs-IT betreut)
- ☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
- ☒ ja (aber nur bei relevanten Risiken – eine Einfache Online- Meldung beim Landesdatenschutz ist möglich)
- ☐ nein

I Datenschutz-Folgeabschätzung (DSFA)
Muss eine DSFA im Unternehmen durchgeführt werden?
- ☐ ja
- ☒ nein (da auch bei Gesundheitsdaten nicht immer ein hohes Risiko bei der Datenverarbeitung besteht)

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
- ☐ ja (beim Einsatz von Überfallschutzkameras)
- ☒ nein (da keine Videoüberwachung durchgeführt wird)

Erläuterungen zu den Anforderungen

A Datenschutzbeauftragter (DSB)

In dem Taxiunternehmen findet in aller Regel keine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten statt, die zu einer Benennungspflicht führt. Es ist daher ein DSB nur zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind

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

B Verzeichnis von Verarbeitungstätigkeiten

Krankenfahrten durchführende Taxi- und Mietwagenunternehmen gehen mit gesundheitsbezogenen Daten um und 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.

- 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. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich sind (z. B. Flyer, Aushang, 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 mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. Dies ist in der Regel bspw. der Fall, wenn nach Abschluss des Fahrauftrages 10 Jahre vergangen sind.

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

F Sicherheit

Um sensible Daten wie z.B. Versichertendaten bei Krankenfahrten bei der Verarbeitung zu schützen, sind neben Standardmaßnahmen weitere Maßnahmen zu treffen. Als Standardmaßnahmen zählen u.a. aktuelle Betriebssysteme, Passwortschutz, regelmäßige Backups und Virenscanner. Daneben sollte der Zugriff auf Versichertendaten nur denjenigen in einem Zugriffs- und Berechtigungskonzept gewährt werden, die diese für ihre Arbeit benötigen. Ein Onlinebuchungsformular muss Ende-zu-Ende transportverschlüsselt werden, weshalb die firmeneigene Webseite über eine SSL-Verschlüsselung verfügen sollte.

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

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. IT-Wartung) 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 einer Krankentransportabrechnung oder Verlust auf dem Postweg), 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 ein Verantwortlicher eine Videoüberwachung (z.B. durch Überfallschutzkameras in den Fahrzeugen) durch, ist eine entsprechende Hinweisbeschilderung erforderlich.

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