Handwerkskammer
Ostwestfalen-Lippe zu Bielefeld

DSGVO – Vorgehen zur Umsetzung Musterbeispiel für Kleinstunternehmen

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 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 Beispiel wird deshalb der vereinfachte Regelfall angenommen.

Kurzbeschreibung des Beispielbetriebs

Der KFZ-Betrieb (freie Werkstatt, Einzelunternehmer) hat 5 Beschäftigte (Inhaber, vier Mitarbeiter in der Werkstatt, eine Beschäftigte in der Auftragsverwaltung / Kundenkontakt Lohnverwaltung, Finanzen, Controling, Steuerangelegenheiten & Jahresabschluss macht ein Steuerberater.
Die Firma betreibt selbst eine Webseite.

Wesentliche Verarbeitungstätigkeiten sollen somit sein:

- Auftrags- und Kundenverwaltung (intern)
- Personalverwaltung (intern)
- Bewerberverwaltung (intern)
- Einkauf und Logistik (intern)
- Lohnabrechnung (extern -> AV)
- Finanzbuchhaltung/ controling (extern -> AV)
- Steuerverwaltung/ Jahresabschluss (extern -> AV)
- Betrieb der Firmenwebseite (extern, über Hosting-Paket eines Web-Dienstleisters -> AV)

Handwerkskammer
Ostwestfalen-Lippe zu Bielefeld

Wesentliche DSGVO-Anforderungen für den Beispielbetrieb

A Datenschutzbeauftragter (DSB) *Muss ein DSB benannt werden?*
☐ ja
☒ nein (da < 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 (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 Nutzerdaten auf Server speichert)
☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
☒ ja (aber nur bei relevanten Risiken – Online-Meldung beim LDB NRW 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)