# DSGVO für kleine Betriebe - diese Datenschutz-Anforderungen sollten mindestens umgesetzt werden

Insbesondere kleine Betriebe leiden zunehmend unter einer eher dünnen Personaldecke, weshalb die team-interne Verteilung weiterer Verantwortung, z.B. für den Datenschutz, immer schwieriger wird. Trotzdem bestimmt auch bei kleinen Betrieben der Umgang mit personenbezogenen Daten das Tagesgeschäft. Demzufolge muss sich die Geschäftsleitung dringend mit dem aktuellen Datenschutzrecht beschäftigen.

## Kunden und Beschäftigte haben umfangreiche Rechte

Kunden und eigene Beschäftigte, deren Namen und persönliche Daten gespeichert und verarbeitet werden, sind grundsätzlich mit konkreten Rechten ausgestattet. Für jeden Betrieb - völlig unabhängig von der Größe - ergibt sich hieraus eine Umsetzungspflicht von konkreten Maßnahmen, damit diese Rechte gewahrt werden. Auch wenn grundsätzlich nicht damit zu rechnen ist, dass kleine Betriebe als erste Institutionen in den Fokus von Datenschutzbehörden oder Abmahnkanzleien rücken, sollten Sie Ihren aus der DSGVO resultierenden Pflichten schnellstens nachkommen. Denn schon ein einziger erboster Kunde könnte andernfalls für rechtliche Scherereien bis hin zu einer Abmahnung sorgen.

Im Ergebnis sind die Anforderungen an den Datenschutz für kleine Betriebe noch überschaubar, außerdem bieten übergeordnete Institutionen wie Landesverbände, Landesdatenschutzbehörden oder Stiftungen Hilfestellungen an, um die DSGVO rechtskonform umzusetzen. Eine Auflistung der wichtigsten Grundlagen und unverzichtbaren Maßnahmen für Geschäftsführer beziehungsweise Datenschutzbeauftragte von kleinen Unternehmen bietet beispielsweise die bayerische Datenschutzaufsichtsbehörde unter https://www.lda.bayern.de/de/kleine-unternehmen.html
Die wesentlichen Punkte hieraus im folgenden Überblick:

## Verantwortlichkeit

Grundsätzlich ist der gesetzliche Vertreter des Unternehmens auch für den Datenschutz verantwortlich, also in der Regel der Geschäftsführer. Zusätzlich muss ein externer oder interner Datenschutzbeauftragter bestellt werden, wenn zehn oder mehr Personen regelmäßig mit personenbezogenen Daten beschäftigt sind. Dabei werden auch Teilzeitstellen als eine volle Person gezählt.

## Verzeichnis von Verarbeitungstätigkeiten

Der Betrieb muss in einem Verarbeitungsverzeichnis aufführen, wo und wie in der EDV oder in analogen Arbeitsvorgängen mittels Papier, personenbezogene Daten erhoben, verarbeitet und Dritten zugänglich gemacht werden. Dazu gehören beispielsweise die Lohn- und Gehaltsabrechnung, die Personalverwaltung, die Kundenverwaltung inklusive Rechnungsdaten, der Versand regelmäßiger Kundennewsletter sowie die Veröffentlichung von Fotos auf der Firmenwebseite.

## 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 Datenschutzgrundverordnung (DSGVO) erfolgt.

## Informations- und Auskunftspflichten

Jedes Unternehmen hat die Pflicht, seine Kunden hinreichend über den Umgang mit deren Daten zu informieren. Darin müssen die Art und Weise, der Zweck und die Dauer der Datenspeicherung erläutert werden. Dies kann über ein gesondertes Merkblatt geschehen, das allen Kunden übergeben wird, oder über einen entsprechenden, leicht einsehbaren Aushang im Kassenbereich des Ladenlokals.

## Einwilligungen der Beschäftigten

Auch wenn bereits im Arbeitsvertrag diverse Einwilligungen der Beschäftigten vorliegen, ist es ratsam, die Beschäftigten noch einmal ausdrücklich einwilligen zu lassen, wenn beispielsweise die Veröffentlichung von personenbezogenem Bild- und Textmaterial auf der Firmenwebseite oder in sozialen Medien beabsichtigt ist.

**Löschung von Daten**

Kunden haben ein Recht darauf, aus dem Kundenverzeichnis gelöscht zu werden, sobald die Geschäftsbeziehung endet. Das setzt natürlich voraus, dass nicht andere Gesetze eine längere Speicherung der Daten ausdrücklich vorschreiben (z.B. Buchhaltungsvorgaben). Hier sollte sich Gedanken darüber gemacht werden, wann eine Löschung der Kundendaten sinnvoll beziehungsweise notwendig ist.

**Sicherheit aller gespeicherten Daten**

Jeder Betrieb sollte auf technisch aktuellem Niveau sicherstellen, dass tatsächlich nur die beauftragten Personen Zugriff auf personenbezogene Daten haben, idealerweise durch ein passwortgeschütztes Rechtesystem. Sonstige Datenspeicherorte wie etwa analoge Karteiablagen müssen angemessen vor unberechtigtem Zugriff geschützt werden. Ebenfalls dringend umzusetzende Standardmaßnahmen sind: Aktuelle Betriebssysteme und Anwendungen, ein Passwortschutz an Rechnern und Handys, regelmäßige Backups und der Einsatz von Virenscannern.

**Auftragsverarbeiter**

Sofern Unternehmen 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.

**Szenario für den Fall von Datenverlust**

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. Dazu sollte im Betrieb ein Prozedere definiert werden. Dies muss eine regelmäßige Abfrage des Datenschutz-Status-Quo beinhalten sowie eine Regelung, wer einen eventuellen Datenverlust in welcher Form wo zu melden hat.

**Datenschutzfolgenabschätzung**

Eine Datenschutzfolgenabschätzung wird nötig, wenn die Datenverarbeitung im Unternehmen ein besonders hohes Risiko für die Rechte einzelner oder aller Kunden bedeutet. Das ist zum Beispiel der Fall, wenn der Betrieb Ratings, Scorings oder sonstige Beurteilungen über Kunden oder Beschäftigte veröffentlicht oder zugänglich macht. In diesem Fall müssen gesonderte Kriterien definiert werden, die den Schutz der Betroffenen möglichst umfassend sicherstellen.

**Videoüberwachung**

Führt ein Betrieb eine Videoüberwachung der öffentlichen Verkaufsräume durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoüberwachung zu informieren.

**Fazit**

Mit diesen Maßnahmen tragen die Verantwortlichen im Unternehmen dafür Sorge, dass wesentliche Bestandteile der DSGVO im Betrieb gemäß der Verordnung umgesetzt werden. Selbstverständlich bedeutet dies allein keine Rechtssicherheit. Daher ist es ratsam, seitens der Geschäftsleitung professionelle Hilfe ins Boot zu holen, um die durchgeführten Maßnahmen regelmäßig auf ihre Rechtssicherheit zu überprüfen.

**Kontakt:**
**Jastus GmbH**
**Andreas Jensch**
**Tel. 04161-736904**
**buero@jastus.de**
**www.jastus.de**