# EU-Datenschutzgrundverordnung (DSGVO) für kleine und mittelständische Unternehmen (KMU)

SMART DATA FORUM

Die EU-Datenschutzgrundverordnung (DSGVO) ist ab 25. Mai 2018 gültig. Alle Unternehmen, einschließlich kleine und mittelständische Unternehmen (KMU), die in der Europäischen Union (EU) ansässig sind oder sich im nicht-EU-Ausland befinden, aber Daten von Personen in der EU verarbeiten, müssen mit der neuen Verordnung konform agieren.

## 1 Führung eines Verzeichnisses aller Datenverarbeitungstätigkeiten

Nur bestimmte KMU werden von Artikel 30, Absatz 1 und 2, befreit. Für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, wird eine Abweichung der Regelung hinsichtlich des Führens eines Verzeichnisses gelten. Ausnahme: Die Verordnung muss trotzdem umgesetzt werden, wenn die von Unternehmen vorgenommene Datenverarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besonderer Datenkategorien bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten einschließt.

## 2 Rechenschaftspflicht für die Einhaltung der Grundsätze des Datenschutzes

Sie müssen jederzeit in der Lage sein, die Einhaltung der Grundsätze des Datenschutzes nachweisen zu können. Auch wenn die Datenverarbeitung rechtmäßig ist, kann es zu Bußgeldern kommen, sofern die notwendigen Nachweise fehlen.

## 3 Neue Vorgaben für Einwilligungserklärungen online und offline

Die Einwilligung im Datenschutz kann in schriftlicher oder elektronischer Form erfolgen. Sie muss freiwillig erteilt und zweckgebunden eingeholt werden. Und sie kann jederzeit widerrufen werden. Die Einwilligungsnachweise müssen jederzeit zur Verfügung stehen.

## 4 Erweiterte Vorgaben für Datenschutzerklärungen auf Webseiten

Die Mindestangaben in der Datenschutzerklärung: Kontaktdaten des Unternehmens; Rechtsgrundlage für die Datenverarbeitung; Speicherdauer; Betroffenenrechte und die Zwecke, zu denen personenbezogene Daten verarbeitet werden. In Einzelfällen müssen auch die folgenden Informationen vorliegen: Kontaktdaten des Datenschutzbeauftragten; die Empfänger, die die Daten erhalten und verarbeiten werden und Verpflichtung zur Bereitstellung der Daten seitens des Betroffenen. Die vollständige Information ist unter Art. 13, Abs. 1 und Abs. 2 zu finden.

## 5 Pflicht zur Datenportabilität

Gemäß Artikel 20 sind Sie verpflichtet (nur bei Einwilligung oder Vertrag), die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu Verfügung zu stellen, wenn die betroffene Person ihre Daten mitnehmen und einem anderen Unternehmen/Anbieter übermitteln möchte.

## 6 Recht auf Vergessenwerden von Nutzerdaten

Wenn personenbezogene Daten für die Zwecke nicht mehr erforderlich sind, für die sie erhoben wurden, müssen sie gelöscht werden. Auch auf Anfrage von Personen müssen in bestimmten Fällen die Daten gelöscht werden.

## 7 Regelungen bei der Auftragsdatenverarbeitung

Sie müssen einen Vertrag mit den Dienstleistern schließen, die personenbezogene Daten in ihrem Auftrag verarbeiten. Die Inhalte des Vertrages sind in Art. 28 DSGVO vorgeschrieben. Sie müssen auch sicherstellen, dass der Auftragnehmer für Sie alle DSGVO Anforderungen gesetzmäßig umsetzt. Auch Alt-Verträge sollten an den Vorgaben des Artikel 28 orientiert werden.

## 8 Prinzip des “One-Stop-Shop”

Diese Regel gilt für Unternehmen, die international tätig sind. Sie ermöglicht es Mittelständlern, sich nur noch mit einer Aufsichtsbehörde befassen zu müssen. Das heißt, bei Verstößen gegen die DSGVO sind die Behörden in dem Land, in dem das Unternehmen den Hauptsitz hat, zuständig.

## 9 Benennung des Datenschutzbeauftragten

Die Benennung eines Datenschutzbeauftragten (DSB) ist für KMU mit weniger als 10 Mitarbeitern freiwillig. Es ist aber empfehlenswert für Unternehmen, die mit großen Datenmengen arbeiten und das Vertrauen des Kunden gewinnen und weiter pflegen wollen, einen DSB zu benennen. Unternehmen, die besondere Kategorien personenbezogener Daten verarbeiten, sind verpflichtet, einen DSB einzustellen. Als besondere Kategorien personenbezogener Daten zählen Informationen zu ethnischer Herkunft, politischen Meinungen, religiösen Überzeugungen, biometrische und genetische Daten, Gesundheitsdaten, sexuelle Orientierung oder Gewerkschaftszugehörigkeit. Die DSB-Stelle muss frei von Interessenkonflikten besetzt werden. Hier muss man auch die Vorhaben des BDSG-neu, § 37 betrachten.

## 10 Meldepflicht von Datenpannen

Im Falle einer Datenpanne muss das Unternehmen die zuständige Aufsichtsbehörde innerhalb von 72 Stunden benachrichtigen. Bei einem hohen Risiko für die betroffenen Personen sind auch diese zu benachrichtigen.

## 11 Höhere Bußgelder

Verstöße gegen der DSGVO können mit Bußgeldern in Höhe von bis zu 4% des gesamten weltweit erzielten Jahresumsatzes oder bis zu 20.000.000 Euro geahndet werden.

## Weiterführende Informationen finden Sie hier:

Selbsteinschätzung-Test: https://www.lda.bayern.de/tool/start.html
Handreichungen für KMU: https://www.lda.bayern.de/de/kleine-unternehmen.html
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: https://www.bfdi.bund.de
Berliner Beauftragte für Datenschutz und INformationsfreiheit: https://www.datenschutz-berlin.de/kurzpapiere.html

Checkliste

# Haben Sie diese Regelungen bereits implementiert?

| | |
|---|---|
| ○ | Hat Ihr Unternehmen einen Datenschutzbeauftragten?<br>Wenn nein, warum nicht?<br>Wenn ja, ist er schon gemäß Art. 37 Abs. 8 DSGVO der zuständigen Aufsichtsbehörde gemeldet? |
| ○ | Haben Sie ein Verzeichnis aller Datenverarbeitungstätigkeiten gem. Art. 30 DSGVO? |
| ○ | Haben Sie einen Auftragsverarbeiter zur Durchführung Ihrer Verarbeitungstätigkeiten?<br>Wenn ja, haben Sie mit Ihrem Auftragsverarbeiter die erforderlichen Vereinbarungen nach Art. 28 Abs. 3 DSGVO bereits abgeschlossen? |
| ○ | Haben Sie Ihre Erklärungen zur datenschutzrechtlichen Information der betroffenen Personen bei der Erhebung der Daten an die Anforderungen gemäß Art. 13 und 14 DSGVO angepasst? |
| ○ | Haben Sie schnelle und effiziente Anwendungen vorbereitet, um Anträge auf Auskunft über die persönlichen Daten gemäß Art. 15 DSGVO vollständig und zeitnah zu erledigen? |
| ○ | Sind Sie darauf vorbereitet, personenbezogene Daten auf Anforderung vollständig zu löschen („Recht auf Vergessenwerden“)? |
| ○ | Haben Sie die nötigen Prozesse vorbereitet, um im Falle einer Datenpanne die Aufsichtsbehörden und die betroffenen Personen innerhalb von 72 Stunden zu benachrichtigen? |
| ○ | Haben Sie die Nutzer bereits bezüglich ihrer Rechte - Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung und Datenportabilität – informiert? |
| ○ | Ist das Budget ausreichend, um die DSGVO umsetzen zu können? |
| ○ | Löschen Sie die Daten, die Sie nicht mehr benutzen. |
| ○ | Wenn Sie Daten erfassen, stellen Sie sicher, dass Sie deutlich ankündigen, welche Daten Sie erheben und wozu diese gesammelt werden. |
| ○ | Aktualisieren Sie entsprechend die Cookie-Regelungen, die AGB und die Datenschutzbestimmungen. |
| ○ | Überprüfen Sie den Datenaustausch mit Dritten. Stellen Sie sicher, dass der Auftragsverarbeiter die Einwilligungen der Nutzer erhalten hat und diese jederzeit zur Verfügung stellen kann. |