

## NEWSLETTER NEUES DATENSCHUTZGESETZ IN DER SCHWEIZ



**Ansprechperson:**  
**Evelyn Hofstetter**  
lic. iur., Rechtsanwältin, Partnerin  
[hofstetter@b-legal.ch](mailto:hofstetter@b-legal.ch)  
+41 (0) 044 266 97 49



**Stefan Jud**  
M.A. HSG, Rechtsanwalt, Partner  
[jud@b-legal.ch](mailto:jud@b-legal.ch)  
+41 (0) 44 266 20 87

### Neues Datenschutzgesetz in der Schweiz per 1. September 2023 – was muss ich als KMU beachten?

Mit der Revision des Schweizer Datenschutzgesetzes ändern sich ab 1. September 2023 wichtige Bestimmungen über die Bearbeitung von Personendaten. Unternehmen müssen in Zukunft verschärfte Regeln beachten – und sollten daher ihre bestehenden Richtlinien und Datenschutzerklärungen bis zum Inkrafttreten des neuen DSG überprüfen und gegebenenfalls anpassen lassen, da bei Verletzung des DSG den Unternehmen hohe Bussen (bis max. CHF 250'000) drohen.

### Um was genau geht es beim neuen DSG?

Zum einen geht es darum, das Datenschutzgesetz an die veränderten technologischen und gesellschaftlichen Verhältnisse (Big Data, Cloud, Social Media, Internet of Things) anzupassen: Die Selbstbestimmung der betroffenen Personen über ihre Daten soll gestärkt werden. Zum anderen wird mit dieser Revision das DSG auf die europäischen Datenschutzregeln abgestimmt: Es soll sichergestellt werden, dass die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt – und die unkomplizierte Datenübermittlung zwischen der Schweiz und der EU auch in Zukunft möglich bleibt.

### Welche KMU sind einem besonders hohen Risiko ausgesetzt, gegen das neue DSG zu verstossen?

Einem besonders hohen Risiko ausgesetzt sind Unternehmen, die grosse Mengen an Personendaten (Personaldossiers, HR Daten etc.) oder besonders schützenswerte Personendaten (Gesundheitsdaten etc.) bearbeiten, Profilings durchführen, Webshops betreiben, automatisierte Einzelentscheide generieren oder generell Personendaten ins Ausland (ausserhalb der EU) übermitteln.

## Mit welchem Aufwand muss ich als KMU rechnen, wenn das neue DSGVO im September 2023 in Kraft tritt?

Der Aufwand hängt davon ab, ob das Unternehmen aufgrund seiner Tätigkeit zu den besonders betroffenen Unternehmen gehört und wie weit es sich bereits an die neuen Entwicklungen angepasst hat. Unternehmen, die bereits DSGVO-konform (EU Richtlinie) sind, haben in der Regel nur wenig Anpassungsbedarf. Wer hingegen nur in der Schweiz tätig ist und bisher noch nichts in Bezug auf die EU DSGVO unternommen hat, sollte so rasch als möglich einen DSGVO Spezialisten kontaktieren und mit einer Gap-Analyse beginnen.

## Was muss ich als KMU beachten, um ab 1. September 2023 die neuen Datenschutzbestimmungen zu erfüllen?

- Es gibt keine Übergangsfrist, d.h. man sollte sich baldmöglichst dieser Angelegenheit annehmen, um per 1. September 2023 DSGVO-konform zu sein
- Überprüfen und Anpassen von Datenschutzerklärungen im Internet (auf Ihrer eigenen Website) und auf Werbe- und Vertragsdokumenten
- Erstellen oder Anpassen von **internen Richtlinien** zur Datenbearbeitung durch die Mitarbeitenden und das Unternehmen. Ein Verstoß gegen das Datenschutzgesetz kann hohe Bussen zur Folge haben
- Sicherstellen, dass **Personendaten gelöscht oder anonymisiert werden**, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind
- Abklären, **in welche Länder Personendaten** bekanntgegeben werden, und Sicherstellen, dass dies nur in jene Länder erfolgt, die einen angemessenen Schutz gewährleisten. Dies gilt auch für die Speicherung auf ausländischen Systemen (Cloud). Der Bundesrat publiziert eine entsprechende Liste (bisher der EDÖB). Soweit die Länder nicht auf dieser Liste aufgeführt sind, dürfen Daten unter bestimmten Bedingungen dennoch exportiert werden, unter anderem nur **mit dem ausdrücklichen (schriftlichen) Einverständnis der Betroffenen**
- Sicherstellen der Datensicherheit im Unternehmen durch **geeignete technische und organisatorische Massnahmen (z.B. Wechsel der Passwörter alle 3 Monate; nur Berechtigte haben Zutritt zu Büroräumlichkeiten und der IT Infrastruktur etc)**. Es gibt für diese sog. TOM Massnahmen Guidelines. Da die Datenübermittlung per E-Mail unsicher ist, sollte zumindest bei besonders schützenswerten Personendaten eine E-Mail-Verschlüsselung zur Verfügung stehen
- Sicherstellen der Datenportabilität, das heisst die Datenherausgabe in einem gängigen elektronischen Format (analog zur DSGVO), wenn die Daten elektronisch und vor allem in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags bearbeitet werden
- Implementieren eines Prozesses, der die fristgerechte Bearbeitung von Betroffenenrechten (z. B. Auskunfts- oder Löschbegehren) gewährleistet
- Implementieren eines Prozesses zur Meldung von Datenschutzverletzungen; Implementieren eines Prozesses zur Datenschutz-Folgenabschätzung, insbesondere wenn eine umfangreiche Bearbeitung von besonders schützenswerten Daten oder eine umfangreiche systematische Überwachung von öffentlichen Bereichen stattfindet oder neue Bearbeitungstechnologien mit hohem Risiko zum Einsatz gelangen

- Die Verträge mit den Auftragsbearbeitern (Dritten) sind zu überprüfen. Insbesondere ist die Aufnahme einer Meldepflicht bei Datenschutzverletzungen und bei der Weitergabe an Unterauftragnehmer empfohlen. Ausserdem muss sich der Verantwortliche vergewissern, dass die Datensicherheit gewährleistet ist
- Ernennen einer Datenschutzberaterin oder eines Datenschutzberaters mit Meldung an den EDÖB (empfohlen). Ihre oder seine Kontaktdaten müssen veröffentlicht werden, z.B. auf der Website des Unternehmens. Gemäss DSGVO ist die Ernennung einer oder eines Datenschutzbeauftragten hingegen zwingend

Sofern Sie den Eindruck haben, dass einer oder einige der oben genannten Punkte bei Ihrem Unternehmen noch nicht umgesetzt sind, dann stehen wir Ihnen gerne zur Verfügung, um eine Gap-Analyse durchzuführen oder Ihnen eine Beratung anzubieten. Die sog. TOM Guidelines (Standard) können wir Ihnen kostenlos zur Verfügung stellen. Zögern Sie nicht uns zu kontaktieren.

