AGVS | UPSA
Auto Gewerbe Verband Schweiz
Union professionnelle suisse de l'automobile
Unione professionale svizzera dell'automobile

SLVASSL
Schweizerischer Leasingverband
Association Suisse des Sociétés de Leasing

Revision des Schweizer Datenschutzgesetzes (DSG) abgeschlossen
Neue Regeln gelten ab 1. September 2023

Mit diversen Mitgliederinformationen seit 2017 haben wir Sie über die laufende Totalrevision des Schweizer Datenschutzgesetzes und die diesbezüglichen Arbeiten des SLV im Rahmen des gemeinsamen Projekts mit dem AGVS informiert. Nun wurde die Revision des Schweizer Datenschutzgesetzes (DSG) abgeschlossen. Am 31. August 2022 hat der Bundesrat die Datenschutzverordnung (DSV) veröffentlicht und das **Inkrafttreten der neuen Regeln per 1. September 2023** beschlossen.

Der SLV und der AGVS haben sich für eine wirtschaftsfreundliche und zugleich EU-kompatible Revision des Datenschutzgesetzes eingesetzt. Das nun vorliegende Gesetz und die dazugehörige Verordnung stimmen zwar in vielen Teilen mit den EU-Regeln überein. Dennoch sind bei der Prüfung und Implementierung des neuen Datenschutz-Setups in einem Unternehmen einige sogenannte «Swiss-Finishes» zu berücksichtigen.

Schweizer Unternehmen haben nun **ein Jahr Zeit, die neuen Regeln umsetzen** – (weitere) Übergangsfristen sind keine vorgesehen.

Nachfolgend stellen wir Ihnen eine Auswahl jener Neuerungen, die Sie als unsere Mitglieder am meisten betreffen dürften, kurz vor. Im Anhang steht Ihnen zudem eine Checkliste mit den einzelnen Aufgaben für die schrittweise Umsetzung der neuen Datenschutzregelungen in Ihrem Unternehmen zur Verfügung.

1. Neue Rollenbezeichnungen (Art. 5 lit. j und k nDSG)

Mit den neuen Regelungen werden die Begriffe des «Verantwortlichen» und des «Auftragsbearbeiters» eingeführt. Für das Verständnis der weiteren Ausführungen – sowie des Gesetzestextes selbst – ist es hilfreich, diese beiden Rollen zu kennen. Als **Verantwortlicher** gilt, wer […] über den Zweck und die Mittel einer Datenbearbeitung entscheidet, also z.B. ein Arbeitgeber für die Bearbeitung von Personendaten seiner Angestellten oder ein Händler für die Bearbeitung von Personendaten seiner Kunden. Als **Auftragsbearbeiter** gilt demgegenüber, wer […] im Auftrag des Verantwortlichen Personendaten bearbeitet, z.B. die Speicherung von Daten auf einem externen Server oder durch Cloud-Dienstleister.

2. Profiling (Art. 5 lit. f. nDSG)

Es wird zwischen normalem «Profiling» und «Profiling mit hohem Risiko» unterschieden. Unter **Profiling** fällt jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, zu analysieren oder vorherzusagen (Art. 5 lit. f nDSG). Das **Profiling mit hohem Risiko** bringt zudem ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich (Art. 5 lit. g nDSG). Profiling **setzt für sich allein keine Einwilligung voraus**, auch nicht bei hohem Risiko (Art. 23 Abs. 2 lit. d nDSG). Es ist jedoch im Zusammenhang mit den Informationspflichten, der Protokollierungspflicht und der Datenschutz-Folgenabschätzung von Bedeutung (vgl. unten).

3. Deutlich erweiterte Informations- und Auskunftspflichten

Die neuen Regelungen verlangen, dass betroffene Personen insbesondere über die Beschaffung von Personendaten **informiert** werden, wobei alle Informationen mitzuteilen sind, die erforderlich sind, damit die betroffenen Personen ihre Rechte geltend machen können und eine transparente Datenbearbeitung gewährleistet ist. Dazu gehören insbesondere die Kontaktdaten des Verantwortlichen, der Bearbeitungszweck und ggf. Empfänger der Personendaten, wenn diese weitergegeben werden (Art. 19 nDSG). Eine vorsätzliche Verletzung dieser Pflicht wird strafrechtlich sanktioniert.

Jede Person kann **Auskunft** darüber verlangen, ob Personendaten über sie bearbeitet werden. Wenn dies der Fall ist, sind ihr alle Informationen mitzuteilen, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Das Gesetz enthält eine entsprechende Aufzählung (Art. 25 nDSG).

4. Automatisierte Einzelentscheidung (Art. 21 nDSG)

Eine automatisierte Einzelentscheidung ist eine Entscheidung, welche ohne menschliches Dazutun aufgrund einer Auswertung von Daten erfolgt (z.B. Konditionen wie Zins, Vertragsdauer, Zahlungsfristen oder Abschluss eines Versicherungs- oder Kreditvertrags etc.) und die für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

Die betroffene Person ist über eine solche automatisierte Einzelentscheidung zu **informieren** und ihr muss die Möglichkeit gegeben werden, ihren **Standpunkt darzulegen**. Die betroffene Person kann – falls sie nicht vorgängig ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt – verlangen, dass eine **Überprüfung durch eine natürliche Person** erfolgt.

Im Rahmen des Auskunftsrechts muss einer betroffenen Person die Logik bekanntgegeben werden, auf der eine automatisierte Einzelentscheidung beruht.

5. Administrative Pflichten

Auch die administrativen Pflichten wurden ausgebaut. Diese umfassen beispielsweise:

- das Führen eines *Bearbeitungsverzeichnisses* (Art. 12 nDSG). Ein Bearbeitungsverzeichnis ist ein Inventar, das die verschiedenen Datenbearbeitungen im Unternehmen enthält. Erfasst werden dabei die unterschiedlichen Zwecke der Bearbeitung (z.B. HR, Marketing etc.) und ihre wesentlichen Rahmenbedingungen. Ausnahmen gelten für Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern (Art. 24 DSV);

- die Erstellung von *Datenschutz-Folgeabschätzungen*, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (Art. 22 nDSG);

- *Meldepflichten* bei Verstössen gegen das Datenschutzgesetz (Art. 24 nDSG und Art. 15 DSV);

- das *Protokollieren* von automatisierten Bearbeitungen besonders schützenswerter Personendaten in grossem Umfang oder Profiling mit hohem Risiko, wenn die ergriffenen präventiven Massnahmen den Datenschutz nicht zu gewährleisten vermögen (Art. 4 DSV); und

- das Erstellen eines *Reglements für automatisierte Bearbeitungen*. Dieses ist zudem regelmässig zu aktualisieren, wenn besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder Profiling mit hohem Risiko durchgeführt wird (Art. 5 DSV).

6. Datensicherheit (Art. 8 nDSG)

Es müssen technische und organisatorische Massnahmen (z.B. Zugriffsrechte, Pseudonymisierung) ergriffen werden, um eine angemessene Datensicherheit zu gewährleisten. Dies beinhaltet auch, dass die Applikationen u.a. so ausgestaltet werden, dass Personendaten standardmässig anonymisiert und/oder nach einer bestimmten Zeit gelöscht werden.

Werden die Personendaten durch einen Auftragsbearbeiter bearbeitet, muss der Verantwortliche sicherstellen, dass auch der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten (z.B. durch sog. Auftragsdatenbearbeitungsverträge, ADV).

Im Zusammenhang mit der Datensicherheit ist ebenfalls erwähnenswert, dass «über die gesamte Bearbeitungsdauer» eine Pflicht zur Überprüfung und gegebenenfalls Anpassung der getroffenen Massnahmen besteht und ein vorsätzlicher Verstoss gegen die Mindestanforderungen an die Datensicherheit sanktionsbewehrt ist.

7. Bekanntgabe von Personendaten ins Ausland

Als Bekanntgabe gilt insbesondere auch die Speicherung der Personendaten auf einem ausländischen System (Server, Cloud), aber auch ein Zugriff durch ein ausländisches Support-Team.

Grundsätzlich dürfen Personendaten ins Ausland bekanntgegeben werden, wenn die Gesetzgebung des Drittstaates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 nDSG). Die Länder, in welchen dies der Fall ist, sind in Anhang 1 der DSV aufgelistet. Bei einer Bekanntgabe von Personendaten in *andere* Staaten – so insbesondere auch in die USA – wird entweder die Anwendung einer konkreten Ausnahmebestimmung oder die Implementierung von alternativen Schutzmassnahmen zur Gewährleistung eines angemessenen Datenschutzes vorausgesetzt (Art. 16 Abs. 2 und Art. 17 nDSG).

8. Sanktionen

Das neue Datenschutzgesetz sieht für die Verletzung bestimmter Pflichten Bussen bis zu CHF 250'000 vor (Art. 60 ff. nDSG). Strafbar sind vorsätzliches Handeln und Unterlassen, nicht jedoch Fahrlässigkeit. Anders als in der EU, wo sich die Sanktionen gegen die Unternehmen richten, wird in der Schweiz grundsätzlich die verantwortliche natürliche Person gebüsst. Das Unternehmen selbst kann nur mit einer Busse bis zu CHF 50’000 gebüsst werden, wenn die Ermittlung der strafbaren natürlichen Person innerhalb des Unternehmens oder der Organisation einen unverhältnismässigen Untersuchungsaufwand mit sich ziehen würde.

Wir empfehlen, zeitnah mit der Umsetzung der neuen Regelungen zu beginnen, damit Ihr Unternehmen am 1. September 2023 DSG-konform aufgestellt ist.

September 2022