DIE POST

Informationen für Unternehmen

zum neuen Schweizer Datenschutzgesetz

Das vorliegende Whitepaper stellt keine verbindliche Rechtsauskunft dar. Wir empfehlen Unternehmen, sich eingehend mit dem neuen Gesetz auseinanderzusetzen und bei Fragen eine rechtliche Beratung in Anspruch zu nehmen.

Das neue Schweizer Datenschutzgesetz tritt per 1. September 2023 in Kraft. Unternehmen sollten jetzt mit den Vorbereitungen beginnen, um die neuen datenschutzrechtlichen Vorgaben einzuhalten und Sanktionen und Bussen zu vermeiden. Doch was gibt es dabei zu beachten? Dieses Whitepaper liefert Antworten auf die wichtigsten Fragen und hilft Unternehmen dabei, das neue Datenschutzgesetz zu verstehen und es mithilfe der richtigen Massnahmen einzuhalten.

Die rasant voranschreitende Digitalisierung stellt Unternehmen vor neue Herausforderungen. Auch deshalb hat der Bundesrat die Revision des Schweizer Datenschutzgesetzes (DSG) beschlossen. Mit der Revision sollen Datenbearbeitungen transparenter gemacht und den Menschen mehr Selbstbestimmung über ihre Daten gegeben werden. Da die Missachtung der datenschutzrechtlichen Vorgaben mit Sanktionen und Bussen geahndet wird, sollten sich Unternehmen rechtzeitig vorbereiten. Nachfolgend werden die zentralen Faktoren erläutert, die Unternehmen bei der Umsetzung des neuen DSG berücksichtigen sollten. Darüber hinaus wird untersucht, welche Auswirkungen das neue DSG auf die digitale Kommunikation hat und wie diese datenschutzkonform erfolgen sollte.

Das Datenschutzgesetz
Die Grundlage für ein modernes Datenschutzrecht in der Schweiz

Was ist das neue DSG?
Das neue Datenschutzgesetz (DSG) ist die Grundlage für ein modernes Datenschutzrecht in der Schweiz. Es tritt per 1. September 2023 in Kraft und ersetzt das alte Bundesgesetz über den Datenschutz. Das revidierte DSG bietet einen Rechtsrahmen, der den Schutz personenbezogener Daten in Anlehnung an die EU-Vorgaben gewährleistet. Davon betroffen sind unter anderem alle Unternehmen (inkl. KMU), die personenbezogene Daten bearbeiten. Die Anforderungen des neuen DSG an die Datenbearbeitung gehen deutlich über die alten hinaus, weswegen Unternehmen Anpassungen vornehmen müssen, um die Vorgaben einzuhalten.

Worum geht es im neuen DSG und warum ist es so wichtig?
Damit die Menschen weiterhin selbst über ihre Daten bestimmen und ihre Persönlichkeit schützen können, muss das DSG an die sich verändernden technologischen und gesellschaftlichen Bedingungen (z. B. Cloud Computing, Big Data, soziale Netzwerke, Internet of Things) angepasst werden. Darüber hinaus muss das DSG an die europäischen Datenschutzregeln angepasst werden. Damit wird die Schweiz voraussichtlich weiterhin als Drittstaat mit angemessenem Datenschutzniveau anerkannt und Schweizer Unternehmen können weiterhin unkompliziert Daten mit EU-Firmen austauschen, ohne dass ihnen Wettbewerbsnachteile entstehen.

Welche Chancen bietet das neue DSG?
Das neue DSG bietet Unternehmen die Chance, ihre Datenschutzpraktiken zu verbessern. Es gewährleistet die Privatsphäre der Kundschaft durch angemessene Sicherheitsmassnahmen und schützt deren Rechte. Dies, indem es die Kundschaft über die Bearbeitung ihrer Daten informiert und ihnen eine Widerspruchsmöglichkeit bietet. Darüber hinaus muss durch das DSG die Datenbearbeitung durch Dritte überwacht werden, damit diese die Datenschutzvorschriften einhalten.

Was ändert sich unter anderem mit dem neuen DSG?

§

1

Neuer Geltungsbereich
Das neue DSG beschränkt sich auf den Schutz der Daten natürlicher Personen und schliesst Daten juristischer Personen nicht mehr ein.

2

Erweiterung der besonders schützenswerten Daten und Aufnahme des Begriffs «Profiling»
Nach dem alten Gesetz sind die religiösen, weltanschaulichen, politischen und gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre sowie die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen geschützt. Mit dem neuen Gesetz zählen auch biometrische Daten (Fingerabdruck, Augen-Iris-Scan) sowie Profiling-Daten als besonders schützenswerte Daten. «Profiling» bezeichnet die automatisierte Bearbeitung von Personendaten, um persönliche Aspekte einer natürlichen Person zu analysieren und vorherzusagen.

3

Berücksichtigung von «Privacy by Design» und «Privacy by Default» im Gesetz
Bei «Privacy by Design» werden von Anfang an datenschutzfreundliche Design- und Architekturprinzipien angewendet, um sicherzustellen, dass die Privatsphäre der Nutzerinnen und Nutzer geschützt ist. Das Ziel ist, Datenschutzrisiken von vornherein zu minimieren. Mit «Privacy by Default» wird sichergestellt, dass bei der Entwicklung von Systemen und Anwendungen datenschutzfreundliche Einstellungen und Funktionen als Standard gelten. So ist die Privatsphäre von Nutzerinnen und Nutzern von Anfang an geschützt und sie können selbst aktiv entscheiden, ob sie mehr Daten preisgeben möchten.

4

Ausbau der Informationspflicht
Neu müssen Unternehmen Betroffene vorzeitig über die Beschaffung ihrer Personendaten informieren. Dies gilt nicht mehr nur für «besonders schützenswerte Daten», sondern für alle Personendaten. So können Betroffene ihre Rechte geltend machen. Das Unternehmen muss der betroffenen Person die Kategorien der bearbeiteten Personendaten mitteilen, sofern die Daten nicht direkt bei der betroffenen Person beschafft werden. Falls Daten ins Ausland übermittelt werden, muss das Unternehmen der betroffenen Person mitteilen, in welchen Staat oder an welches internationale Organ die Daten gesendet wurden. Um diese Informationspflicht zu erfüllen, können die Daten beispielsweise. proaktiv und einfach zugänglich über die Unternehmenswebsite bereitgestellt werden.

5

Dokumentationspflicht
Unternehmen müssen nicht mehr nur die Datensammlung dokumentieren, sondern neu ein Verzeichnis über die gesamten Datenbearbeitungsprozesse führen, das alle relevanten Informationen zu den bearbeiteten Personendaten enthält. Um dies zu tun, müssen die Identität des Verantwortlichen, der Bearbeitungszweck sowie die Kategorien der betroffenen Personen, die bearbeiteten Personendaten, Empfängerinnen und Empfänger, Aufbewahrungsdauer und Massnahmen zur Gewährleistung der Datensicherheit angegeben werden. Falls die Daten ins Ausland übermittelt werden, müssen zudem der Staat und die Garantien zum Datenschutz angegeben werden.

Wichtig
Im Gegensatz zur DSGVO (siehe Box) richten sich Bussen und Sanktionen gegen natürliche Personen (nicht gegen juristische Personen). Dazu zählen Leitungspersonen wie CEO, CTO, CFO, aber auch Fachkräfte ohne Leitungsfunktion wie Datenschutzbeauftragte. Unternehmen können sich dagegen nicht versichern. Verletzt eine natürliche Person in einem Unternehmen das neue DSG, werden Sanktionen gegen diese Person ergriffen.

6

Meldung bei Datensicherheitsverletzung
Verletzungen der Datensicherheit müssen unter gewissen Umständen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden.

7

Datenschutz-Folgenabschätzung
Unternehmen müssen neu eine schriftliche Datenschutz-Folgenabschätzung erstellen, wenn die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten von betroffenen Personen darstellt und kein Ausnahmegrund gegeben ist.

8

Verschärfung der Sanktionen
Bei Missachtung des Datenschutzrechts drohen Sanktionen und Bussen von bis zu 250 000 Franken. Der EDÖB kann ein Untersuchungsverfahren eröffnen und Verfügungen erlassen. Ausserdem sind auch zivilrechtliche Klagen möglich. Für die Sanktionsumsetzung sind die kantonalen Strafverfolgungsbehörden zuständig.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) regelt den Schutz personenbezogener Daten der Menschen in der EU. Sie gilt seit 25. Mai 2018 und ersetzte die Datenschutzrichtlinie (DSRL) von 1995. Die DSGVO stellt strengere Anforderungen an den Schutz personenbezogener Daten und sanktioniert Verstösse stärker. Zu den wichtigsten Bestimmungen der DSGVO gehören die Regeln für den Umgang mit personenbezogenen Daten sowie die Rechte der betroffenen Personen.

Welche Massnahmen gilt es umzusetzen?

Unternehmen müssen unter anderem Folgendes beachten:

Bestandsaufnahme der Bearbeitungen von Personendaten

Gemäss dem neuen DSG müssen Unternehmen bestimmte Informationen bereitstellen. Dazu zählen die Kontaktdaten der für die Datenbearbeitung verantwortlichen Person, der Bearbeitungszweck sowie etwaige Datenempfänger. Die Unternehmen müssen aber auch die Rechte von betroffenen Personen achten und unter Umständen die Einwilligung für die Bearbeitung ihrer Daten einholen. Somit muss das Unternehmen über die Datenbearbeitungen Bescheid wissen. Dies schliesst auch die Datenübermittlungen in andere Länder oder an weitere Personen mit ein. Empfehlenswert ist daher, eine Bestandsaufnahme aller Personendaten zu machen, wobei das neue gesetzliche Verzeichnis der Bearbeitungstätigkeiten als Orientierungshilfe dienen kann.

Verzeichnis der Bearbeitungstätigkeiten führen

Das neue DSG schreibt Verantwortlichen und Auftragsbearbeitenden vor, ein Verzeichnis ihrer Bearbeitungstätigkeiten anzulegen. Das gilt grundsätzlich für alle Unternehmen, wobei der Bundesrat für Firmen mit weniger als 250 Mitarbeitenden Ausnahmen vorsehen kann (Art. 12 Abs. 2 revDSG). Um ein solches Verzeichnis zu erstellen, müssen sämtliche Bearbeitungen von Personendaten in einem Unternehmen identifiziert und systematisch zusammengetragen werden. Da dies sehr aufwendig ist, sollte dieser Prozess frühzeitig angegangen werden, insbesondere wenn noch keine entsprechenden Verzeichnisse geführt wurden.

Risikobewertung

Um das datenschutzrechtliche Risiko für die Verantwortlichen zu bewerten, wird jeder Prozess der Bearbeitung von Personendaten untersucht. Dafür werden mögliche Gefahren in Bezug auf Eintrittswahrscheinlichkeit des Risikos und dessen Auswirkungen abgeschätzt und klassifiziert. Eine hohe Risikobewertung besteht vor allem dann, wenn viele Personendaten bearbeitet werden, mehrere Parteien involviert sind und die Daten besonders schützenswert sind.

Bewusstsein schaffen

Alle Mitarbeitenden aller Stufen in jedem Unternehmen sollten über das Thema Datenschutz aufgeklärt werden. Sie müssen wissen, welche strafbewehrte Verantwortung sie bei der Bearbeitung von Personendaten tragen. Praktische Beispiele hierfür sind der Versand von sensiblen Dokumenten per E-Mail oder die Erfassung der Vor- und Nachnamen von Besucherinnen und Besuchern durch Empfangsmitarbeitende: Bereits durch den Versand, die Dokumentation und Archivierung dieser Informationen werden Personendaten bearbeitet.

Transparenz als wesentlicher Aspekt

Die Transparenz bei der Datenverarbeitung ist auch beim revidierten DSG ein wesentlicher Aspekt. Dazu kommt, dass Betroffene vorgängig über die Datenerhebung informiert werden müssen. Um diese Anforderungen zu erfüllen, müssen beispielsweise Datenschutzerklärungen erstellt oder aktualisiert werden. Diese sollten sowohl auf der Unternehmenswebseite als auch in der physischen Korrespondenz zur Verfügung gestellt werden.

IT-Sicherheit gewährleisten

Unternehmen müssen gegebenenfalls ihre IT-Systeme und Software anpassen, um das neue Gesetz einzuhalten. Dazu müssen technische und organisatorische Massnahmen ergriffen werden, um Cyberangriffe, Datendiebstahl und anderweitige Datenverluste zu verhindern bzw. zu minimieren.

Interne Prozesse definieren

Um gesetzeskonform auf Betroffenenanfragen oder Datensicherheitsverletzungen reagieren zu können, müssen interne Prozesse mit klaren Massnahmen und Fristen für Mitarbeitende definiert werden. Hierbei ist insbesondere festzuhalten, wer welche Schritte ergreifen muss.

Verträge prüfen

Damit Unternehmen nach Inkrafttreten des neuen DSG ihre Compliance sicherstellen können, sollten frühzeitig alle Verträge und Abkommen mit der Kundschaft, mit Lieferanten, Dienstleistern und Arbeitnehmenden auf mögliche Anpassungen überprüft werden.

Informieren und an Schulungen teilnehmen

Um über die Auswirkungen des neuen DSG informiert zu bleiben, sollte man die Website der Datenschutzbehörde besuchen, Blogs lesen und an Schulungen teilnehmen.

Mit der E-Mail-Verschlüsselungslösung IncaMail der Schweizerischen Post können Unternehmen schützenswerte Daten verschlüsselt und nachweisbar versenden – einfach und sicher. Die verschlüsselten Nachrichten sind durch mehrere Sicherheitsebenen geschützt und können nur vom Empfänger eingesehen werden. So kommunizieren Unternehmen in der digitalen Welt sicher und datenschutzkonform. Mit IncaMail können nicht nur Unternehmen, sondern auch die Mitarbeitenden, die Nachrichten versenden, geschützt werden.
Mehr über IncaMail erfahren Sie hier: www.post.ch/incamail

Fazit

Das neue Datenschutzgesetz (DSG) ist ein wichtiger Schritt hin zu einem modernen Datenschutz. In diesem Whitepaper wurden die wichtigsten Punkte des neuen DSG erläutert, Chancen aufgezeigt und erklärt, dass Unternehmen frühzeitig Massnahmen ergreifen sollten, um den Datenschutz zu gewährleisten. Darüber hinaus sollten Firmen Sicherheitsmassnahmen bei der digitalen Kommunikation treffen, um personenbezogene Daten zu schützen. Die elektronische Datenübermittlung muss daher sicher sein. Ein Beispiel aus der Praxis ist hierfür der Versand von sensiblen Daten per E-Mail.

Immer häufiger verschicken Unternehmen Offerten, Verträge, Rechnungen oder Lohnabrechnungen per E-Mail statt per physischer Post. Was für Unternehmen praktisch und effizient ist, birgt jedoch Gefahren. Denn E-Mails sind nicht nur wenig geschützt, sie werden unter Umständen auch den Anforderungen des Datenschutzgesetzes nicht gerecht. Unternehmen brauchen deshalb eine zuverlässige Lösung, um sensible Informationen sicher per E-Mail auszutauschen. **Wir empfehlen deshalb, elektronisch versendete Daten zu verschlüsseln. So reduzieren Sie Risiken.**