versaLex AG
Schaffhauserstrasse 125
8057 Zürich
kontakt@versalex.ch
0041 43 499 59 00

Revidiertes Datenschutzgesetz ab September 2023

Sind Sie vorbereitet? Ein kurzer Check für KMU

Die Revision des Schweizer Datenschutzgesetzes auf den 1. September 2023 ist in aller Munde – und wohl auch in den Köpfen der Inhaber und Geschäftsführer von KMUs. Im revidierten Gesetz findet eine weitgehende Annäherung an die europäische Datenschutz-Grundverordnung (DSGVO) statt, welche schon seit knapp 5 Jahren gilt. Der Inhalt der DSGVO wurde aber nicht für alle Belange als Vorbild genommen. Damit bleibt die Umsetzung der Datenschutzanforderungen für Schweizer KMU nicht immer einfach. Vorab aber eine kleine Entwarnung: Wer bereits vor 5 Jahren Massnahmen zur Umsetzung der DSGVO getroffen hat, muss diese nicht über den Haufen werfen. Mit ein paar Anpassungen ist auch die Konformität mit dem revidierten Schweizer Datenschutzgesetz gegeben.

Das in den Unternehmen wohl am heissesten diskutierte Thema ist die Einführung der neuen Bussenregelung, wonach nicht etwa das Unternehmen, sondern die darin arbeitenden Privatpersonen mit Bussen von bis zu CHF 250'000 zur Verantwortung gezogen werden können.

Viele Schweizer KMU fragen sich heute, wie sie sich mit dem Thema Datenschutz auseinandersetzen sollen und was es für sie konkret zu unternehmen gilt. Denn: Nicht alle Unternehmen müssen die gleichen Vorkehrungen treffen. Der vorliegende Artikel soll ihnen eine Hilfe bei dieser Einschätzung sein.

Die to do Liste

Schaffen Sie sich Übersicht – Bearbeitungsverzeichnis ja oder nein?

Unter gewissen Umständen haben Sie ein sogenanntes Bearbeitungsverzeichnis zu erstellen, in welchem Sie verschiedene Informationen über die Datenbearbeitung in Ihrem KMU festhalten. Diese Pflicht ist mit einem beachtlichen Aufwand verbunden. Um zu prüfen, ob das Erstellen von einem solchen Verzeichnis Pflicht für Ihr KMU ist, müssen Sie sich die folgenden Fragen stellen:

1. In Ihrem KMU arbeiten mehr als 250 Personen (Vollzeitstellen)
2. Ihr KMU bearbeitet besonders schützenswerte Personendaten (vgl. Know-how am Ende)
3. Ihr KMU verarbeitet Personendaten in einer Weise, welche ein hohes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt

Können Sie all diese Fragen mit gutem Gewissen mit «Nein» beantworten, dann benötigen Sie kein Bearbeitungsverzeichnis. Dies wird vor allem bei kleineren KMUs zutreffen, welche ausschliesslich im B2B Bereich tätig sind und gar nie oder nur im geringen Masse mit besonders schützenswerten Personendaten in Berührung kommen. Trotzdem müssen Sie die Antworten zu den Fragen periodisch überprüfen, um allenfalls zu einem späteren Zeitpunkt ein Verzeichnis zu erstellen.

Haben Sie auch nur eine der Fragen mit «Ja» beantwortet, so haben Sie ein Bearbeitungsverzeichnis zu erstellen. Das Bearbeitungsverzeichnis muss Ihnen einen Überblick über sämtliche Applikationen und Prozesse geben, bei denen in Ihrem KMU personenbezogene Daten bearbeitet werden.

Wichtigster Inhalt des Bearbeitungsverzeichnisses ist unter anderem die Auflistung folgender Informationen:

- Bearbeitungszweck;
- Beschreibung von Kategorien betroffener Personen (z.B. Konsumenten, Arbeitnehmer)
- Beschreibung von Kategorien bearbeiteter Personendaten (z.B. Wohnadressen, Salär, besonders schützenswerte Personendaten);
- Kategorien der Empfänger;
- Angabe des Staates und der Garantien, sofern Daten ins Ausland bekannt gegeben werden.

Für das Erstellen des Bearbeitungsverzeichnisses benötigen Sie die Unterstützung Ihres IT-Teams genauso wie der einzelnen Verantwortlichen in den Bereichen Verkauf, Einkauf, HR, Finanzen etc. Diese können Ihnen sagen, welche Personendaten Ihr KMU wo und wie bearbeitet.

Machen Sie sich die Angelegenheit aber nicht schwerer als sie ist: Eine Excelliste, die sämtliche Bearbeitungen auflistet und die nötigen Informationen enthält, reicht hier völlig aus.

Wir raten auch Unternehmen mit weniger als 250 Mitarbeitern dazu, ein zumindest rudimentäres Verzeichnis der Datenbearbeitungen zu führen, sozusagen ein «Bearbeitungsverzeichnis light». Dieses Verzeichnis hilft dabei zu prüfen, ob die Informationspflicht über Datenbearbeitungen, die von allen Unternehmen zu beachten ist, eingehalten ist. Im Übrigen hilft dieser Überblick auch bei der Beantwortung von Auskunfts- oder anderweitigen Begehren von betroffenen Personen.

INFORMIEREN, INFORMIEREN, INFORMIEREN!

Eine grosse Veränderung bringt das neue Datenschutzrecht in Sachen Informationspflicht mit sich. Neu sind die Betroffenen über jede Bearbeitung ihrer Personendaten im Voraus zu informieren. Die Verletzung dieser Pflicht kann bei vorsätzlichem Handeln, wie eingangs erwähnt, gebüsst werden.

Die von der Datenbearbeitung betroffenen Personen in Ihrem KMU können Sie grundsätzlich in die folgenden beiden Kategorien einteilen:

1. Mitarbeitende (interne Kategorie): Proaktive Information mittels einer internen Datenschutzerklärung (z.B. im Personalreglement)
2. Konsumenten, Kunden, Websitenutzende, Lieferanten etc. (externe Kategorie): Information mittels einer externen Datenschutzerklärung

Wissen Ihre Mitarbeitenden heute nicht, wie, wo und welche ihrer Daten Sie bearbeiten, dann müssen Sie zwingend proaktiv darüber informieren. Haben Sie bis heute noch keine Datenschutzerklärung auf Ihrer Website, welche für externe Personen frei zugänglich ist, so haben sie auch dies dringend nachzuholen.

Verfügen Sie schon seit längerem eine externe und interne Datenschutzerklärungen, so empfiehlt sich eine Überprüfung, mittels welcher Sie die Aktualität sicherstellen.

Keine Weitergabe von Daten an Dritte ohne Vertrag

Es ist kaum denkbar, dass ein Unternehmen heute noch ohne Dienstleister auskommt, welche in irgendeiner Weise Daten Ihrer KMUs bearbeiten. Bereits das nicht selbst gehostete HR-Tool oder die Auslagerung der Buchhaltung an Drittunternehmen führt automatisch zu einer Datenbearbeitung durch Dritte (sog. **Auftragsdatenbearbeiter**, vgl. dazu näheres Know-how am Ende). Dem Drittunternehmen dürfen Sie die Daten Ihres KMUs nur dann weitergeben, wenn Sie mit diesen einen Vertrag geschlossen haben, welcher die Datenbearbeitung in geeigneter Weise regelt (sog. Datenbearbeitungsvereinbarungen oder DPA, data processing agreements). Mit diesen Vereinbarungen stellen Sie u.a. sicher, dass das Drittunternehmen nur erlaubte Datenbearbeitung vornimmt, den Zugriff auf die Daten schützt, die Daten nicht (ins Ausland) weitergibt oder ohne Vorabgenehmigung weitere Datenbearbeiter einsetzt, etc.

Kein Transfer ins Ausland ohne Absicherung

Personendaten dürfen ins Ausland bekanntgegeben werden, sofern im entsprechenden Land ein genügend angemessener Schutz der Daten besteht. Eine Liste der Staaten mit angemessenem Datenschutz befindet sich im Anhang zur Verordnung über den Datenschutz (Datenschutzverordnung, DSV). Datenstransfers z.B. ins europäische Umfeld sind unproblematisch.

Schwieriger gestaltet sich die rechtliche Lage bei Datentransfers ins sog. «unsichere» Ausland, wozu z.B. die USA, Indien oder China gehören. Wenn Sie Daten in eines der besagten Länder transferieren, sind weitere Massnahmen zu treffen (z.B. Abschluss von **Standardvertragsklauseln**, siehe dazu Know-how am Ende). Alternativ ist im Einzelfall die Einwilligung der Betroffenen für den Transfer ins Ausland einzuholen.

Indem ein Grossteil der Daten elektronisch gespeichert wird, werden Daten rasch weitergegeben. Befindet sich z.B. der Speicherort von Daten Ihres KMUs im Ausland (ebenfalls rasch der Fall bei z.B. Cloud-Servern), so haben Sie diese schon ins Ausland weitergegeben. Einige amerikanische Dienstleister bieten bereits heute Lösungen an, bei denen die Daten ausschliesslich auf europäischen Servern abgelegt werden. Datenschutzrechtlich ist das Problem damit zwar aufgrund der weiterhin bestehenden Möglichkeit eines Zugriffs des amerikanischen Unternehmens auf die Cloud-Inhalte nicht gelöst, aber sicherlich massiv entschärft.

Prüfen Sie, ob sie eine Datenschutz-Folgenabschätzung benötigen

Beabsichtigen Sie eine Datenbearbeitung, durch die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person entsteht, so haben Sie vorgängig eine Datenschutz-Folgenabschätzung vorzunehmen. Dies ist insbesondere dann der Fall, wenn Sie neue Technologien verwenden oder wenn Art, Umfang, Umstände und/oder Zweck der Bearbeitung ein hohes Risiko mit sich bringen. Für die Vornahme der Datenschutz-Folgenabschätzung sowie für die daraus folgende Risikobewertung wird der Beizug eines externen Experten empfohlen.

Legen Sie einen Prozess für die Beantwortung von Betroffenenbegehren und für Vorfälle fest

Betroffene können mit Begehren an Sie gelangen: Sie haben unter anderem ein Recht auf Auskunft, auf Löschung, auf Berichtigung etc. Mit Ausnahme des Rechts auf Datenherausgabe und -übertragung in einem gängigen elektronischen Format sind dies keine neuen Rechte. Wichtig ist aber, dass Sie wissen, wie Sie auf ein allfälliges Begehren reagieren müssen. Auskunftsbegehren müssen innerhalb von 30 Tagen beantwortet werden. Wenn Sie also bereits einen konkreten Prozess festgelegt haben, können Sie in der Folge umso gelassener sein. Im Prozess sind folgende Aspekte zu regeln:

1. Überprüfung der Berechtigung zur Stellung des Begehrens
2. Festlegung interner Verantwortlichkeiten
3. Form und Inhalt der Beantwortung.

Einen Prozess und die Klärung von Verantwortlichkeiten ist ebenfalls notwendig, wenn es zu einer **Datenpanne** (sog. «Data breach», siehe Know-how am Ende) kommt. Solche Datenpannen sind gemäss neuem Datenschutzrecht dem EDÖB «so rasch als möglich» zu melden, wenn sie zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Unter Umständen ist auch die betroffene Person zu informieren und z.B. aufzufordern. Da bei einer Datenpanne schnelles Handeln gefordert ist, lohnt es sich, wenn schon vorab die Verantwortlichkeiten und die Prozesse geklärt sind.

…und trotzdem ist es gut zu wissen, dass nicht alles schwieriger wird:

- Grundsätzlich bleibt es beim System, wonach Datenbearbeitungen von Personendaten erlaubt sind, solange die **Grundsätze des Datenschutzes** (hierzu Know-how am Ende) eingehalten sind.
- Eine Einwilligung zur Datenbearbeitung wird nur in wenigen Fällen vorausgesetzt, insbesondere eben dann, wenn die Grundsätze nicht eingehalten werden können.
- Eine Datenbearbeitung durch Dritte bleibt weitgehend gleichermassen möglich und ein Transfer ins Ausland wird nicht grundsätzlich erschwert.
- Die Strafbestimmungen kommen nur zum Tragen, wenn vorsätzlich gehandelt wird, nicht jedoch bei fahrlässigem Handeln. Trotzdem lohnt es sich, keine Strafverfahren zu riskieren.
- Es gibt weiterhin keinen Zwang, einen Datenschutzbeauftragten (unter neuem Recht neu der «Datenschutzberater») zu bestimmen. Wer einen offiziellen Datenschutzbeauftragen bezeichnet, hat unter anderem den Vorteil, dass der Gang zum EDÖB bei einer Datenschutzpanne unterbleiben kann.

Kleines Datenschutz Know-how:

Personendaten: Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (z.B. Name, Adresse, Geburtsdatum, IP-Adresse etc.). Juristische Personen sind unter dem neuen Datenschutzgesetz nicht mehr geschützt. Nur wer Personendaten bearbeitet, untersteht dem Datenschutzgesetz. Nun handelt es sich aber bereits bei Mitarbeiterdaten um Personendaten, zum Teil sogar um «besonders schützenswerte» Personendaten. Genauso sind auch Emailadressen und Kontak-

tinformationen von Mitarbeitern der Geschäftspartner oder Geschäftskunden Personendaten gemäss Datenschutzgesetz. Aus diesem Grund hat sich grundsätzlich jedes KMU die Frage zu stellen, wie sie mit den Anforderungen des Schweizer Datenschutzrechts umgehen sollen. Diese sind – je nach Art der Tätigkeit – unterschiedlich: von KMU z.B. im Industrie- und Gewerbebereich, die in erster Linie mit B2B Partnern arbeiten und keinerlei sensitive Daten bearbeiten, sind sie geringer als bei KMU mit Daten von Privatkunden (B2C).

Besonders schützenswerte Personendaten:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;
- Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie;
- genetische Daten;
- biometrische Daten, die eine natürliche Person eindeutig identifizieren;
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen;
- Daten über Massnahmen der sozialen Hilfe.

Grundsätze der Datenbearbeitung:

- Ausschliesslich rechtmässiges Bearbeiten
- Bearbeitung nach Treu und Glauben und Einhaltung der Verhältnismässigkeit
- Zweckmässigkeit: nur zu bestimmtem für die betroffene Person erkennbaren Zweck
- Vernichtung oder Anonymisierung, wenn für Bearbeitungszweck nicht mehr erforderlich
- Richtigkeit und Vollständigkeit der Daten ist zu überprüfen

Können diese Grundsätze der Datenbearbeitung nicht eingehalten werden oder ist zweifelhaft, ob diese in einem bestimmten Fall eingehalten sind, ist die Bearbeitung von Daten nicht per se zu unterlassen. Wichtig ist in diesen Fällen, dass bei der betroffenen Person eine Einwilligung eingeholt wird.

Bearbeiten: Darunter fällt jede Art von Bearbeitung, z.B. auch der Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

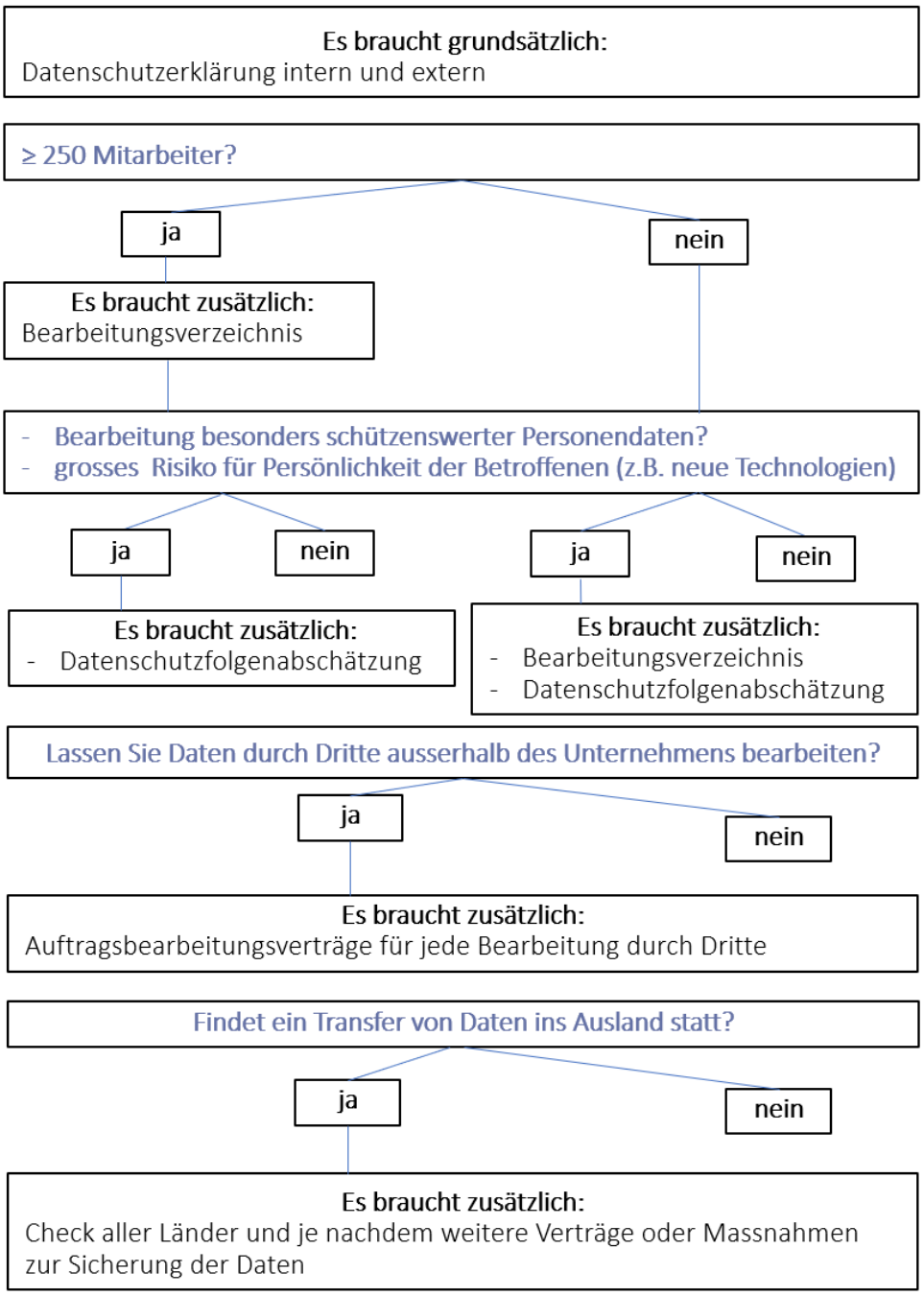
Auftragsbearbeiter: Die Bearbeitung von Personendaten kann einem Auftragsbearbeiter übertragen werden (z.B. Outsourcing HR in einem HR-Tool). Als Auftragsbearbeiter gelten nur jene, die Daten so bearbeiten, wie es der Verantwortliche selbst tun dürfte. Der Auftragsbearbeiter hat sich daher genau an die Zweckbestimmung zu halten und darf die Daten nicht für eigene Zwecke verwenden. Eine Auftragsbearbeitung ist zudem dann nicht zulässig, wenn eine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet, die Daten durch jemand anderen bearbeiten zu lassen.

Standardvertragsklauseln: Sogenannte Standard Contracting Clauses (SCC) bieten die Möglichkeit, Personendaten in ein als unsicher geltendes Ausland zu transferieren. Durch die Vereinbarung von solchen Klauseln kann ein angemessener Schutz durch Vertrag gewährleistet werden. Eines der bekannten Vertragswerke, das vom EDÖB anerkannt wird, sind die Standardvertragsklauseln der EU gemäss dem Beschluss der Europäischen Kommission. Die meisten grösseren Internet-Dienstleister machen solche Standardvertragsklauseln bereits von vornherein zum Bestandteil ihrer Verträge. Wenn ein Unternehmen diese nicht anbietet, sollten Sie beim Abschluss eines Vertrages vorsichtig sein und diesen Umstand hinterfragen. Im Juni 2021 wurden neue Standardvertragsklauseln der Europäischen Kommission erlassen. Unternehmen, die Standardvertragsklauseln einsetzen, hätten per

Ende 2022 bereits sämtliche Verträge anpassen sollen. Wer noch alte in Gebrauch hat, sollte sich in einem allerersten Schritt um diese Aktualisierung kümmern.

Datenpanne: Sogenannte Data Breaches sind Verletzungen der Datensicherheit. Es geht darum, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Zu denken ist hier an Hackerangriffe, versehentlich öffentlich gemachte oder gelöschte Kundendaten etc.

ENTSCHEIDBAUM FÜR DIE NOTWENDIGEN VORKEHRUNGEN



AUTORINNEN:

Dr. RA Eva Maissen
T: +41 43 499 59 01
eva.maissen@versalex.ch

Eva hat jahrelange Erfahrung in der rechtlichen Beratung von Unternehmen und Kunden. Ihr liegen pragmatische Lösungen und sie ist überzeugt, dass auch rechtliche Dokumente verständlich, prägnant und so kurz wie möglich gehalten werden sollten. Sie kommuniziert mit Kunden offen und zielorientiert und kommt so schnell zum gewünschten Ergebnis.

Beratungsschwerpunkte

Beratung in den für ein Unternehmen relevanten Rechtsbereichen wie allg. Vertragsrecht (insb. AGB), Arbeitsrecht, Compliance (u.a. Datenschutzrecht), Wettbewerbsrecht, Gesellschaftsrecht, etc. (exkl. Steuerrecht und Strafrecht)

RA Karin Steiner
T: +41 43 499 59 02
karin.steiner@versalex.ch

Karin bringt ein breites unternehmerisches Verständnis mit und hat echtes Interesse an den Zielen ihrer Kunden. Ihre Kommunikation findet jederzeit auf Augenhöhe statt, was eine einfache und transparente Zusammenarbeit ermöglicht. Durch die pragmatische und lösungsorientierte Unterstützung erhalten die Kunden gewinnbringende Resultate.

Beratungsschwerpunkte

Beratung in den für ein Unternehmen relevanten Rechtsbereichen wie allg. Vertragsrecht, Arbeitsrecht, Compliance (u.a. Datenschutzrecht), Wettbewerbsrecht, Gesellschaftsrecht, etc. (exkl. Steuerrecht und Strafrecht)