

Revidiertes Datenschutzgesetz – revDSG

Das revidierte DSG im KMU – welche Daten muss ich künftig schützen und wie?



Dass es ein Datenschutzgesetz gibt, ist uns bestens bekannt. Was aber bedeutet das auf September 2023 angekündigte revidierte DSG? Welcher spezifische Handlungsbedarf besteht für uns als KMU? In diesem Artikel wenden wir uns nicht als Fachexperten für Datenschutz an unsere Akzente-Leser. Vielmehr geht es darum, einige auf eigener Erfahrung basierende Anregungen an unsere Leser weiterzugeben. Denn selbstverständlich befassen wir uns als Treuhandfirma sehr eingehend mit diesen Fragen. Ihre Daten sollen bei uns sicher auf-

bewahrt und der Schutz soll gewährleistet sein.

Das revidierte Datenschutzgesetz (revDSG) soll Anfang September 2023 vom Bundesrat in Kraft gesetzt werden. Theoretische Grundlagen zum Thema finden wir in Hülle und Fülle. Was heisst dies alles aber für die konkrete Umsetzung? Was muss ein KMU vorkehren, und wo Prioritäten setzen? Die folgenden Ausführungen sind als Impulse gedacht, als praktische Hinweise, wie Sie die Thematik angehen können.

Missverstehen ist menschlich!

Egal wie viele digitale Kommunikationsmittel wir einsetzen: Ob wir uns in der Sache verstehen – oder eben missverstehen – hängt noch immer von uns selbst ab. Gerade im KMU, wo wir meist gut aufeinander eingespielt sind, unterschätzen wir leicht, wie wichtig eine deutliche Kommunikation ist. Wir geben beispielsweise kurz und bündig einen Auftrag weiter und meinen, das erwünschte Ergebnis sei klar. In der Folge heisst es dann ganz unverhofft: «Das habe ich aber anders verstanden» oder «Das war nicht so gemeint» – was meist weder emotional noch sachlich erspriesslich ist. Reinhard Sprenger, der bekannte Führungsexperte und Autor, hat den Krux der zwischenmenschlichen Kommunikation in seinen Worten auf den Punkt gebracht: «Am Anfang war das Wort, gleich darauf kam das Missverständnis.» Unser Gehirn ist nämlich so konstruiert, dass wir von Natur aus nicht automatisch das Gleiche wie unser Gegenüber wahrnehmen. Rational gesehen ist es deshalb klüger, vom potenziellen Missverstehen auszugehen, respektive sich bewusst zu sein, dass gegenseitiges Verstehen aktiv geschaffen werden muss. Wann immer also das Wort «selbstverständlich» auftaucht, kann es sinnvoll sein, kurz zu hinterfragen: Sieht es der oder die andere wirklich gleich? Dieser Ministopp lohnt sich auf jeden Fall. Es gibt weniger unerwünschte Diskussionen oder Missverständnisse. Zudem macht der Austausch mehr Freude und dieses gegenseitige Zusammenspiel wirkt sich positiv auf die Ergebnisse aus.



Andreas Okle

Andreas Okle
Geschäftsführender Partner

Welches sind die relevanten Neuerungen?

Das revDSG erfasst nur noch die Daten von natürlichen Personen. Unternehmen, d.h. juristische Personen, werden davon nicht mehr erfasst. Diese sind anderweitig geschützt und geregelt. Aufgrund der Internationalität von Schweizer Firmen haben viele KMU schon Bekanntschaft mit der DSGVO gemacht, der Datenschutz-Grundverordnung der EU, welche seit Mai 2018 in Kraft ist und für die auf EU-Gebiet tätigen Akteure anwendbar ist. Im Gegensatz zur DSGVO verfolgt das schweizerische revDSG das Prinzip, dass alle Datenverarbeitungen erlaubt sind, mit Ausnahme der besonders schützenswerten Daten (siehe dazu die Auflistung auf S. 4). Werden diese schützenswerten Daten für die Verarbeitung zwingend verwendet, dürfen sie zudem ohne besondere Einwilligung bearbeitet werden. Zum Beispiel benötige ich für die Bekanntgabe der Konfession bei der Verarbeitung der Lohndaten keine explizite Zustimmung. Das Gleiche gilt für die Erstellung der Steuererklärung oder die Bearbeitung eines Kundenauftrags. In jedem anderen Fall ist eine explizite Zustimmung notwendig. Zu beachten ist, dass auch das Empfangen und das Speichern von Daten bereits als «Bearbeitung» gilt.

Die Einwilligung zur Bearbeitung von Daten kann auch in Zukunft über die AGB eingeholt werden.

Folgende weitere Neuerungen sind zu beachten:

- Personendaten müssen durch angemessene technische und organisatorische Massnahmen (sogenannte TOMs) gegen unbefugtes Bearbeiten geschützt werden. Was jedoch heisst angemessen? Hier gilt es, laufend

Trend

Ein Kabel für Minimalisten

Sechs Ladekombinationen in einem einzigen Kabel



Kabelsalat, zu langsame Übertragungsraten, zu viel verschiedene oder zu kurze Kabel – je mehr technische Geräte wir haben, je mehr können uns Computer-accessoires ganz schön nerven. Das Tessiner Unternehmen *Rolling Square* hat sich zum Ziel gesetzt, perfekte Computer-accessoires anzubieten.

Das incharge®XL Kabel ist sozusagen ein universelles Kabel für alles. Es verfügt über 6 verschiedene Ladekombinationen, mit denen praktisch jedes Gerät mit jeder Stromquelle geladen werden kann. Mit seinen zwei INPUTS (USB und USB C) und den drei OUTPUTS (USB, Micro USB und Lightning) löst es einen grossen Teil jedes Kabelsalats und erlaubt damit, blitzschnell von einem Gerät zum nächsten zu wechseln – vom Laptop zum Tablet zum Handy zum Kopfhörer zur Boombox und vieles mehr. Die Adapter können abgenommen werden und natürlich gibt es auch eine Schutzkappe für die Stecker. Zudem sind sie so konstruiert, dass sie auch bei groben Handyschutzhüllen funktionieren. Die Stecker sind bis zu 135 Grad schwenkbar und die Anschlüsse sind vollständig aus einer Zink-Aluminium-Legierung, was sie besonders stabil macht. Nicht nur zum Laden, auch zum Datenübertragen ist es bestens geeignet.

Das Kabel ist auch enorm schnell. Das Chipset, welches das Innenleben des Kabels ausmacht, leistet bis zu 100 W Ultra Fast Charging, kann also auch ein Notebook locker laden. Gleichzeitig erlaubt das Kabel Datenübertragungsraten von 480 Mbps / 60 Mbps.

Es gibt das Kabel in drei Längen: von 30 cm zum Verbinden von Notebook und Mobile Devices über 2 Meter bis hin zu langen 3 Metern. Und dies in den drei Farben schwarz, weiss und gelb. Dazu kommen bei der 3 Meter Variante zwei Cable Organizer und eine elastische Silikonhülle.

Das incharge®XL Kabel ist seit 2014 die 11. erfolgreiche Kampagne von *Rolling Square* auf Kickstarter und indiegogo. Auch sonst hat Rolling Square eine ganze Menge sehr innovativer und praktischer PC-Accessoires im Shop. Lohnt sich, dort mal reinzuschauen.

www.rollingsquare.com

Intern

Herzlich willkommen in unserem Team



Seit November 2021 arbeitet **Elvira Chopard** als diplomierte Sozialversicherungs-Expertin in unserem Unternehmen und ist für den Bereich Sozialversicherungen zuständig. Zuvor konnte sie in ähnlichen Funktionen bereits einige Jahre wertvolle Erfahrungen sammeln. Mit Elvira möchten wir den vielfältigen sowie zunehmend komplexen Bereich Sozialversicherungen weiter stärken und ausbauen.



Seit November 2021 unterstützt **Carola Vescovo** als Treuhandexpertin unser Buchhaltungsteam. Sie führt nationale wie auch internationale Mandatsbuchhaltungen. Neben den klassischen Treuhandarbeiten verfügt sie als zugelassene Revisionsexpertin auch über mehrjährige Erfahrungen im Bereich Wirtschaftsprüfung.



Folgende Dokumente stellen wir Ihnen auf www.caminada.com/akzente zur Verfügung:

- Präsentation von Andreas Okle Kongress Treuhand 2022 (Auszug)
- Übersicht Aufbewahrungsfristen
- www.datenrecht.ch
- www.DSAT.ch (Datenschutz Self Assessment Tool)
- Inhalt Datenverarbeitungsverzeichnis
- Unterschied DSGVO und revDSG



www.datenrecht.ch



www.DSAT.ch
Datenschutz Self Assessment Tool

Herzlichen Dank

Das Akzente wird seit Jahren durch Mitarbeitende der **Stiftung zuwebe** verpackt und versendet. Herzlichen Dank für die wertvolle Arbeit!



>> Fortsetzung von Seite 2

die Erfordernisse im Auge zu behalten, selbst wenn es keine expliziten Vorschriften gibt. Beispielsweise war die Multifaktorauthentifizierung (MFA) vor einigen Jahren noch die Ausnahme, heute ist es ein erforderlicher Standard. Auch eine professionelle Lösung zur Verschlüsselung von Mails gehört in diesen Bereich.

- Im Gegensatz zur DSGVO der EU müssen in der Schweiz im Unternehmen keine Datenschutzbeauftragten definiert werden. Es kann freiwillig ein Datenschutzberater ernannt werden, welcher dann aber dem EDÖB (Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragter) gemeldet werden muss.
- Bis jetzt war eine DSG-Erklärung auf der Website gemäss CH-Recht nicht erforderlich, neu ist sie zwingend. Stellen Sie demnach sicher, dass auf Ihrer Website eine aktuelle DSG-Erklärung publiziert ist. Sie muss jedoch auf der Website nicht automatisch aufpoppen und bestätigt werden. Weil dies unter der europäischen DSGVO-Verordnung aber zwingend ist, wurde es auch in der Schweiz auf den meisten Websites implementiert.

Die Übersicht behalten

Da sich die Umsetzung des DSG wie beschrieben fortwährend dahinzieht, ist es aus Gründen der Effizienz wichtig, die Klarheit und die Übersicht zu behalten. Am besten von Beginn an!

a) Das Bearbeitungsverzeichnis und den Datenkatalog erstellen

Dazu empfehlen sich die folgenden vier Schritte:

- Erstellen Sie einen Datenkatalog für Ihr Unternehmen. Welche Datenkategorien (Adressdaten, Lohndaten,

Zu den besonders schützenswerten Daten gehören:

- Biometrische Daten
- Genetische Daten (Daten, die eine natürliche Person eindeutig identifizieren)
- Religiöse, weltanschauliche, politische Ansichten
- Gesundheit, die Intimsphäre
- Zugehörigkeit zu einer Rasse oder Ethnie
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen
- Daten über Massnahmen der sozialen Hilfe

CRM-Daten etc.) haben wir im Haus?

- Ergänzen Sie die Liste mit den Datenspeicherorten. Wo genau sind diese Daten und weitere Kundendaten gespeichert? (z.B. on premise, Cloud, Drittanbieter).
- Erweitern Sie die Tabelle mit den spezifischen Bearbeitungstätigkeiten (z.B. speichern, verarbeiten, versenden).
- Lokalisieren Sie die besonders schützenswerten Personendaten.

b) Katalog der Datensicherheitsmassnahmen

Sie haben bestimmt schon verschiedene Massnahmen zur Gewährleistung der Datensicherheit implementiert. Erstellen Sie einen Katalog der Massnahmen und Lösungen, welche bereits aktiv sind. So lässt sich einerseits erkennen, was schon erledigt ist, und andererseits, wo noch Handlungsbedarf besteht. Gleichzeitig finden Sie sich schnell zurecht, wenn frühere Massnahmen im Verlauf der Zeit angepasst werden müssen.

Die Archivierung der Personendaten

Ein zentrales Element sind die Archivierung und die sichere Aufbewahrung der Personendaten. Wie haben Sie diese gelöst? Es muss für das Unternehmen ein Archivierungskonzept mit einer entsprechenden Systematik erarbeitet und implementiert werden. Dazu gehört auch eine präzise Angabe, wie lange die Daten aufbewahrt werden müssen. Diesbezüglich gilt die Regel: Die gesetzlichen Aufbewahrungsfristen (Legal Holds) gehen immer vor, auch wenn es sich um besonders schützenswerte Daten handelt. Es kann Sie niemand zum Löschen von Daten zwingen, die Sie für die Erfüllung der gesetzlichen Aufbewahrungspflichten benötigen (vgl. dazu die Hinweise zu den Aufbewahrungsfristen im «Cami-Service» in diesem Akzente).

Und sollte es dennoch passieren

Sollte es in Ihrem Unternehmen trotz aller Vorsichtsmassnahmen zu einem Datenleck kommen, empfehlen wir Ihnen, die Meldepflichten an den EDÖB ernst zu nehmen. Das revDSG kennt keine verbindliche Frist wie z.B. die europäische Datenschutzverordnung (DSGVO 72h). Das heisst, wenn eine Cryptolocker-Falle zugeschnappt hat, müssen Sie davon ausgehen, dass Ihre Daten bereits kopiert sind und im Darknet angeboten werden, bevor sie auf Ihrem Rechner verschlüsselt wurden.

Die Sache ernst nehmen – und realistisch bleiben

Eines möchten wir zum Schluss betonen: Der Anspruch, zu jedem Zeitpunkt hundert Prozent DSG-compliant zu sein, ist kaum realistisch. Vielmehr geht es darum, die laufenden Entwicklungen zu kennen, die bestehenden Lösungen entsprechend immer wieder zu überprüfen und wo nötig nachzubessern. Es ist ein Weg der kleinen Schritte, dafür konsequent und beharrlich!