



Max Wellerdieck
Rechtsanwalt & Öffentlicher Notar



Selina Grass
Rechtsanwältin & Öffentliche Urkundsperson

Arbon
+41 71 466 30 30

St.Gallen
+41 71 230 30 30

Weinfelden
+41 71 633 30 30

Wil
+41 71 925 30 30

Winterthur
+41 52 346 30 30

«MILESTONE BY SARTORIAL»

Mit dem «milestone by sartorial» informieren wir Sie zu praxisrelevanten und aktuellen Themen aus verschiedensten Wirtschafts- und Rechtsgebieten.

XV. DATENSCHUTZ ALS RISIKOFAKTOR FÜR DAS UNTERNEHMEN

NEUES DATENSCHUTZGESETZ – WAS KMU BEACHTEN MÜSSEN - NACHTRAG

MEHR DATENSCHUTZ: WARUM JETZT?

Die Gesellschaft wird in Bezug auf Personendaten immer sensibler. Mittels Datenspuren können eine Person, ihre Interessen und ihre Vorlieben einfach identifiziert werden. So erstellte Persönlichkeitsprofile werden kommerziell genutzt. Die Politik nimmt das Schutzbedürfnis auf, indem die Bearbeitung von Personendaten gesetzlich immer stärker reguliert wird. Angefangen hat dies vor einigen Jahren in der EU mit der Datenschutz-Grundverordnung (DSGVO). Die Schweiz zieht nun mit ihrem eigenen **neuen Datenschutzgesetz** nach, das definitiv auf den 1. September 2023 in Kraft tritt. Dieses betrifft Sie auf jeden Fall, während die Relevanz der DSGVO in der Schweiz jeweils abgeklärt werden muss. Wir wollen Ihnen deshalb hier rechtzeitig kurz und knapp das Wichtigste zum neuen Gesetz mit auf den Weg geben.

WELCHE DATEN? WAS HEISST BEARBEITEN?

Das Gesetz regelt die *Bearbeitung* von *Personendaten*. Personendaten sind dabei alles, was sich vage mit einem bestimmten Menschen verknüpfen lässt. Auch die IP-Adresse oder Adresse eines Wohnblocks kann ein Personendatum darstellen. Alles, was Sie mit diesen Daten machen, gilt als Bearbeitung, auch nur das Anzeigen auf einem Bildschirm oder das Abspeichern auf einer Festplatte. Gehen Sie deshalb davon aus, dass Sie in Ihrem Unternehmen einiges an Personendaten bearbeiten.

WAS MUSS ICH FÜR MEIN KMU WISSEN?

Informationspflicht: Vorab ist eine aktuelle **Datenschutzerklärung** notwendig. Fragen Sie sich deshalb zuerst: Ist so eine Erklärung vorhanden und auf Ihrer Website für jeden Nutzer einfach zugänglich?

Dokumentationspflicht: Jedes Unternehmen muss **vor neuen Datenbearbeitungen eine Folgenabschätzung** über die Risiken für die betroffenen Personen vornehmen. Unternehmen mit mehr als 250 Mitarbeitenden müssen darüber hinaus ein **Verzeichnis über alle Datenbearbeitungen** (bspw. die Kundenkartei, die Lohnbuchhaltung, die Website etc.) führen und auf Verlangen der Aufsichtsbehörde vorlegen können.

Auskunftspflicht: Stellen Sie sicher, dass Sie Anfragen einer betroffenen Person **innerhalb von 30 Tagen vollständig und kostenlos beantworten** können. Die Daten müssen auf Verlangen hin berichtigt oder gelöscht werden können.

Datensicherheit: Wie steht es um die **technischen Sicherheitsmassnahmen** rund um Computer und Internet in Ihrem Unternehmen? Virenschutz, Firewall, Passwortschutz: Sind alle Programme auf dem aktuellen Stand? Verfügen sämtliche Computer über einen sicheren Passwortschutz? Bestehen **organisatorische Sicherheitsmassnahmen**? Bspw. regelmässige Schulungen der Mitarbeitenden über die Gefahr von Datenverlust bzw. -diebstahl durch Hacking oder Phishing-Mails.

Archiv: Überlegen Sie sich, was Sie an Personendaten wirklich brauchen und brauchen dürfen: Speichern Sie nur, was nötig ist. Löschen Sie Personendaten, welche nicht mehr benötigt werden oder mutmasslich falsch sind. Stellen Sie sicher, dass Sie alle Datenbestände kontrollieren. Liegt vielleicht noch ein Magnetband mit veralteten Kundenlisten in Ihrem Banksafe? Durch ein **sauberes Archiv** können Sie viele Risiken stark minimieren. Gleichzeitig erleichtert es Ihnen, der erwähnten Auskunftspflicht nachzukommen.

Datenschutzklausel in Verträgen mit Dritten: Mit dem neuen Datenschutzgesetz sind Sie für die Personendaten verantwortlich, gerade auch dann, wenn Sie diese an Dritte weitergeben. Hält sich ein Vertragspartner oder Dienstleister nicht an das neue Gesetz, können Sie dafür haftbar gemacht werden. Fragen Sie sich daher: Sind Ihnen sämtliche Vertragspartner und Dienstleister bekannt? Denken Sie bspw. an die E-Mail-Service-, Telefonservice-, Cloudspeicher- oder Cloud-Software-Anbieter, Bürogerätevermieter, Treuhanddienstleister, die IT-Fernwartung oder Freelancer. **Sind die Datenbearbeitung und die Datensicherheit vertraglich geregelt (Datenschutzklausel)?** Bei Bekanntwerden von wiederholten Datenlecks oder systematischen Datenschutzverletzungen durch den Geschäftspartner sollte die Zusammenarbeit schnellstmöglich beendet werden. Hier ist auch an entsprechende Kündigungsrechte bei der Vertragsgestaltung zu denken.

Hat der Dritte seinen Geschäftssitz im Ausland ausserhalb der EU, ist für ein datenschutzkonformes Vertragswerk unbedingt eine Fachperson beizuziehen. Allgemeingültige Aussagen lassen sich dazu nicht mehr machen.

WER IST VERANTWORTLICH?

Grundsätzlich müssen betroffene Personen eine Verletzung des Datenschutzgesetzes selbst geltend machen. Eine unzulässige Datenbearbeitung stellt einerseits eine **Persönlichkeitsverletzung** dar. Die betroffene Person kann dabei gegen alle an der Verletzung Mitwirkenden gerichtlich vorgehen. Auch das rein passive (jedoch bewusste) Tolerieren von Datenschutzverletzungen durch Mitarbeitende stellt eine Mitwirkung dar und führt zur Haftung von Unternehmen und Organen, nebst dem entsprechenden Mitarbeitenden. Aufgrund der grösseren Liquidität dürfte jedoch hauptsächlich das Unternehmen mit Klagen konfrontiert werden. Andererseits kann die betroffene Person einen **Strafantrag** stellen. Eine Verletzung der vorgenannten Bestimmungen

kann neu mit **Bussen bis zu CHF 250'000** bestraft werden. Die Bussenhöhe fällt im Vergleich zum Ausland eher tief aus, da in der Schweiz der Mensch und nicht das Unternehmen gebüsst werden soll. Es haften also jene Personen, welche aufgrund ihrer Stellung und ihrer Befugnisse tatsächlich Einfluss auf das Unternehmen ausüben können, bspw. die Verwaltungsräte. Das Unternehmen wird nur gebüsst, wenn die handelnde Person aufgrund mangelnder Organisation nicht oder nur mit unverhältnismässigem Ermittlungsaufwand festgestellt werden kann.

EXKURS: EINWILLIGUNG NOTWENDIG?

Die Einwilligung der betroffenen Person in die Bearbeitung ihrer Daten ist – im Gegensatz zum EU-Recht – grundsätzlich weiterhin nicht notwendig.

Als Faustregel für eine zulässige Datenbearbeitung gilt: **Sie dürfen Daten zwar ohne Einwilligung der betroffenen Person, aber nur zu einem ganz bestimmten Zweck und nur so lange bearbeiten, als dies notwendig ist.** Sammeln und Speichern von Daten auf Vorrat ist nicht erlaubt.

Übrigens: Die weitverbreiteten Cookie-Anfragen auf Webseiten sind in der Schweiz nicht nötig. Es besteht jedoch eine Informationspflicht, bspw. in der Datenschutzerklärung.

FAZIT

Es ist wichtig, dass Sie sich frühzeitig mit dem aktuellen Datenschutz in Ihrem Unternehmen auseinandersetzen, um rechtzeitig Massnahmen ergreifen und umsetzen zu können. Das neue Datenschutzgesetz tritt nämlich ohne Umsetzungsfrist in Kraft und Datenschutzverstösse könnten danach sofort geahndet werden.

Prüfen Sie deshalb jetzt Ihre internen Prozesse, Richtlinien, Verträge und Datenschutzerklärungen auf die Konformität mit dem neuen Gesetz. Der Datenschutz sollte fortan in Ihrem Risikomanagement seinen festen Platz finden.

Haben Sie Fragen zu unseren Ausführungen? Wir freuen uns, Sie mit einer massgeschneiderten Beratung fit für das neue Datenschutzgesetz zu machen.

Herzlichen Dank für Ihr Vertrauen.

Ihr Sartorial-Team
St.Gallen, Weinfelden, Wil, Zürich