Merkblatt – Umgang mit Daten und Datenschutz

KMU-Unternehmer stehen vor der Herausforderung, ihre geschäftliche Tätigkeit so zu gestalten, dass Konflikte mit dem Datenschutzgesetz möglichst vermieden werden können.

Mit dem Inkrafttreten des neuen Schweizerischen Datenschutzgesetzes und der zugehörigen Verordnung im Herbst 2023 wurde im Kreis der davon betroffenen Unternehmer ein grosses Mass an Unsicherheit geschaffen. Hier finden Sie einen kurzen Überblick dazu, was die heute gültige Rechtslage verlangt, und wie der Umgang allenfalls etwas entspannter gestaltet werden kann.

Vorab empfiehlt sich ein Blick auf die Ziele des Datenschutzgesetzes: Sein Zweck besteht nicht darin, die unternehmerische Tätigkeit unnötig zu erschweren, sondern im Schutz der Persönlichkeit der – natürlichen – Personen, deren Daten bearbeitet werden. Daraus ergibt sich, dass nur die Daten von *natürlichen* Personen Gegenstand des neuen Schweizerischen Datenschutzgesetztes sind. Daten von juristischen Personen sind nicht im Fokus dieses Gesetzes (der Schutz deren Persönlichkeit erfolgt durch andere Gesetze).

Schutz der Persönlichkeit bedeutet, dass die betroffene Person insbesondere vor einem unbeschränkten oder verdeckten Datamining geschützt werden soll. Der Einzelne soll erkennen können, wenn seine Daten erfasst werden und er soll nicht mit unerwarteten und für ihn nicht absehbaren Datenverarbeitungen konfrontiert werden.

Die technische Entwicklung hat es mit sich gebracht, dass es heute sehr einfach geworden ist, Daten in grossen Mengen zu sammeln und zu analysieren. Die KI-Technologien werden es mit sich bringen, dass die Analyse noch wesentlich einfacher und effizienter werden dürfte. So ist es heute technisch problemlos möglich, die Besucher eines Ladens zu identifizieren und zu analysieren, wann sich wer wie lange und wo aufhält, was studiert und was letztlich gekauft wird. Aus einer Vielzahl an sich belangloser Daten kann so – ähnlich einem Mosaik – ein Profil der Persönlichkeit einer Person erstellt werden, das mehr über diese Person aussagt, als selbst deren nächste Angehörige wissen.

Das sind die technischen Möglichkeiten, welche eine gesetzliche Regelung notwendig und auch sinnvoll machen.

A Handlungsbedarf und konkrete Massnahmen

Beim Umgang mit Daten im Unternehmensalltag sollten einige zentrale Grundsätze eingehalten werden:

1. Schaffen Sie eine Übersicht über die in Ihrem Unternehmen erhobenen Personendaten und sensibilisieren Sie Ihre Mitarbeitenden

Um überhaupt beurteilen zu können, welche Datenbearbeitungen in Ihrem Unternehmen täglich erfolgen, werden Sie ganz unabhängig von der Grösse ihres Betriebs nicht darum herumkommen, sich eine Übersicht dazu zu verschaffen, «welche Personendaten zu Ihnen gelangen, wie, und von wem sie zu welchem Zweck bearbeitet werden». Zur «Bearbeitung» gehört letztlich jeder Umgang mit Daten, der gesamte Kreis von der Erhebung über die Aufbewahrung, die Veränderung bis zur Löschung der Daten. Der Kreis der Personen, deren Daten hier relevant sind, umfasst alle entsprechenden (natürlichen) Personen, einschliesslich der eigenen Mitarbeiter.
Es ist sinnvoll, alle Beteiligten für den sorgfältigen Umgang mit Daten zu sensibilisieren.

➔ Wir unterstützen Sie bei der konkreten Umsetzung der sich aufdrängenden Handlungen mit entsprechenden Checklisten, damit dieser Prozess strukturiert werden kann und führen auf Wunsch auch Informationsveranstaltungen in Ihrem Betrieb durch.

2. Rechtmässigkeit der Datenbeschaffung

Die Beschaffung von Daten muss rechtmässig sein und darf nicht gegen Treu und Glauben verstossen. Dass es nicht zulässig ist, jemanden auszuspionieren, scheint selbstverständlich. Die technische Entwicklung bringt es aber mit sich, dass die Möglichkeiten, für den Betroffenen nicht erkennbar Daten zu erfassen, zunehmen. Der korrekte Unternehmer vermeidet Schwierigkeiten, wenn er mit Zurückhaltung agiert.

➔ Wir helfen bei der kritischen Überprüfung der Datenbeschaffung und bestehenden Datenverwaltung.

3. Transparenz

Schaffen Sie Transparenz über die erfassten Daten und den Zweck, zu welchem diese erfasst werden. Wenn dies aus den Umständen klar hervorgeht – aber wirklich nur dann bzw. insoweit dieser aus den Umständen hervorgeht – ist es nicht notwendig, dem Betroffenen den für diesen ja erkennbaren Umstand der Datenerfassung und der Verwendung explizit nochmals zu erläutern.
Bei einer Mangelmeldung durch eine Mieterin in einer Neuüberbauung dient die Weitergabe deren Koordinaten (Personendaten!) an den für die Mangelbehebung aufzubietenden Unternehmer dem Zweck der Mängelbehebung und damit schlussendlich der Vertragserfüllung durch die Vermieterschaft. Es dürfte hingegen über diesen Zweck hinausgehen, diese Angaben an mehr oder weniger zufällig ausgewählte Personen weiterzuleiten (heikel: ganze E-Mail-Chroniken «im cc» an sämtliche Beteiligten eines Bauprojekts). Im Zweifel schadet es nicht, auch selbstverständliche und für den Betroffenen erkennbare und von ihm erwartete Datenbearbeitungen explizit mitzuteilen.
Zur Transparenz der Datenbearbeitung gehört, dass beschaffte Daten nicht über die erkennbaren oder mitgeteilten Zwecke hinaus Verwendung finden dürfen. Nicht zuletzt ist für die Information die geeignete Form zu finden.

➔ Wir unterstützen Sie bei der Analyse der Verarbeitung von Daten und bei der Formulierung der erforderlichen Informationen gegenüber den Betroffenen.

4. Verhältnismässigkeit

Sammeln Sie keine Daten, die für den jeweiligen Zweck nicht notwendig sind, sondern hinterfragen Sie kritisch, was sinnvoll ist.

➔ Wir unterstützen Sie beim Analysiere der Menge und Art der verarbeiteten Daten und suchen mit Ihnen nach Lösungen, um Datenberge zu vermeiden.

5. Datensparsamkeit

Der Umstand, dass Daten einfach zu sammeln und billig zu verarbeiten sind, kann dazu verleiten, allzu exzessiv Daten zu sammeln und überaus lange aufzubewahren. Das ist zu vermeiden, stattdessen sollte nicht mehr gesammelt und auch nicht länger aufbewahrt werden, als für den konkreten, dem Betroffenen erkennbaren Zweck angebracht. Beispiele: Moderne Schliesssysteme ermöglichen es, zu erfassen, mit welchem Schlüssel - und damit auch von welcher Person – zu welcher Zeit eine bestimmte Tür benutzt wurde. Solche Daten können ohne grosse Kosten längere Zeit gespeichert und analysiert werden. Es besteht aber im Normalfall kein legitimer Bedarf danach, zu analysieren,

welche Personen beispielsweise zu welchen Uhrzeiten eine Mietliegenschaft betreten haben. Die persönliche Neugier des Hauswarts taugt auch nicht als Rechtfertigung dazu.
Auf die Erfassung von Daten, die offensichtlich nicht notwendig sind, sollte von Anfang an verzichtet werden. Das gilt beispielsweise im Personalwesen, wo schon auf die Erfassung von Daten, die für die fragliche Tätigkeit nicht von Relevanz sind, von Anfang an sinnvollerweise verzichtet wird.

➔ Wir erarbeiten mit Ihnen die notwendigen Strukturen zur angemessenen gesetzeskonformen Aufbewahrung und Löschung der verschiedenen Datenkategorien.

6. Datensicherheit

Wer Daten bearbeitet, insbesondere wer sie aufbewahrt, hat dafür zu sorgen, dass diese sich nicht selbständig machen und abhandenkommen, beispielsweise indem nicht autorisierten Dritten durch zu lockere Sicherheitsmassnahmen die Möglichkeit geboten wird, Zugang zu Daten zu erhalten. In der Datenschutzverordnung sind zum Thema der Datensicherheit weitergehende Regeln statuiert. Dazu gehört insbesondere der Grundsatz, dass nur jene Personen Zugriff auf Daten haben sollen, welche sie zur Erfüllung ihrer Aufgaben benötigen. Dazu sind insbesondere technische und organisatorische Massnahmen zu treffen, welche den Zugang zu, aber auch die Integrität entsprechender Daten regeln und gewährleisten.
Die entsprechenden Regeln sind nicht starr, vielmehr ist dabei jeweils auf die Art der bearbeiteten Daten, die Art und Weise der Bearbeitung und die Schwere drohender Gefahren Rücksicht zu nehmen. Die zur Datensicherheit ergriffenen Massnahmen haben sich schliesslich nach dem Stand der Technik und nicht zuletzt auch nach den dafür anfallenden Kosten zu orientieren. Da all diese Aspekte sich im Laufe der Zeit verändern, sind die getroffenen Massnahmen periodisch zu überprüfen.

➔ Wir unterstützen Sie bei Bedarf beim Auffinden von Anlaufstellen mit dem entsprechenden technischen Know-How.

7. Umgang mit besonders schützenswerten Personendaten und Profiling mit hohem Risiko

Als besonders schützenswerte Personendaten gelten insbesondere Daten über religiöse, politische oder weltanschauliche Ansichten, Daten über die Gesundheit oder Intimsphäre, aber auch die Angehörigkeit zu einer Rasse oder Ethnie, genetische Daten generell, biometrische Daten, soweit diese eine Person eindeutig identifizieren sowie schliesslich Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen sowie Massnahmen der sozialen Hilfe.
Solche besonders schützenswerten Personendaten erfahren auch vom Datenschutzgesetz einen besonderen Schutz, indem deren Bearbeitung an sich nur beim Vorliegen einer ausdrücklichen Einwilligung zulässig ist und die Weitergabe an Dritte grundsätzlich eine Persönlichkeitsverletzung darstellt.
Als Profiling mit hohem Risiko gilt die automatisierte Bearbeitung von Personendaten, die zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, und damit ein hohes Risiko für die Persönlichkeit oder die Grundrechte einer Person darstellt.

➔ Wir unterstützen Sie beim Umgang mit besonders schützenwerter Personendaten, wenn diese für Ihre Tätigkeit notwendig sind.

B Rechtfertigungsgründe

Verstösst jemand gegen die obigen, in Art. 6 - 8 DSG statuierten Datenbearbeitungsgrundsätze, bearbeitet er Personendaten entgegen dem ausdrücklich erklärten Willen der betroffenen Person oder gibt er einem Dritten besonders schützenswerte Personendaten bekannt, so stellt dies eine Persönlichkeitsverletzung dar, die grundsätzlich unzulässig ist

Als Rechtfertigungsgründe in Frage kommen in erster Linie überwiegende private oder öffentliche Interessen. So weit ein Gesetz die Öffentlichkeit gewisser Daten statuiert, was beispielsweise bei gewissen Handelsregisterdaten der Fall ist, so stellt auch dies ein Rechtfertigungsgrund dar, was im Ergebnis zur Folge hat, dass es auch entgegen dem ausdrücklichen Willen einer betroffenen Person zulässig sein kann, entsprechende Daten zu bearbeiten.

Gesetzliche Anforderungen dürften als Rechtfertigungsgründe in sehr vielen Fällen von erheblicher praktischer Bedeutung sein, verlangen doch insbesondere die Regeln des Arbeitsrechts die Bearbeitung zahlreicher Daten, wie beispielsweise die Erfassung der Arbeitszeit oder die Bearbeitung von Daten, welche für die Erfüllung zahlreicher Arbeitgeberpflichten erforderlich sind.
Auch die Vorschriften über die Führung und Aufbewahrung von Geschäftsbüchern und Belegen, stellen sehr weitgehende Forderungen, welchen kaum nachgekommen werden kann, ohne die entsprechende Bearbeitung von Personendaten.

Rechtfertigungsgründe sind nicht nur relevant, wenn es um die Rechtfertigung einer Persönlichkeitsverletzung geht, sie sind auch von Relevanz bei der Frage, ob überhaupt ein Verstoss gegen die Regeln der Art. 6 - 8 DSG vorliegt. Das ist beispielsweise der Fall im Zusammenhang mit der Bestimmung in Art. 6 Abs. 4 DSG, die fordert, dass Daten zu vernichten oder zu anonymisieren sind, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

C Informationspflicht und Auskunftsrecht

Das neue Datenschutzgesetz statuiert in Art. 25 ein sehr weitgehendes Auskunftsrecht, welches es dem Betroffenen ermöglichen soll, Kenntnisse von den über ihn bearbeiteten Daten und die Art und Weise der konkreten Bearbeitung zu erhalten. Eine eigentliche Informationspflicht gilt aber nach Art. 19 DSG bereits bei der Beschaffung von Daten und beschränkt sich nicht nur auf das Faktum der Datenerfassung, sondern beinhaltet auch die aktive Bekanntgabe des Verantwortlichen, des Bearbeitungszwecks und gegebenenfalls der Empfänger, wenn Daten an Dritte weitergegeben werden sollen. Dazu bietet sich in vielen Fällen an, diese Informationen z.B. in einer Datenschutzerklärung auf der Homepage zu fassen.
Das Datenschutzgesetz soll nicht Grund für sinnlose Pflichtübungen sein und so ist insbesondere dann eine aktive Information nicht erforderlich, wenn die betroffene Person über die entsprechenden Informationen bereits verfügt. Kenntnis über entsprechende Informationen liegen insbesondere dann vor, wenn ein Betroffener die entsprechenden Daten aktiv liefert. Die Person des Datenschutzverantwortlichen hingegen ist dem Betroffenen im Normalfall aber nicht bekannt und eine entsprechende Mitteilung ist daher geboten. Dasselbe gilt dann, wenn der Zweck der Datenbearbeitung weiter gehen soll, als erkennbar ist. Diesfalls ist auch der entsprechende Bearbeitungszweck mitzuteilen.

➔ Wir helfen Ihnen bei der Beurteilung der Frage, ob eine Informationspflicht besteht und wie weit diese geht, sowie bei der Erarbeitung einer effizienten Vorgehensweise zwecks angemessener Beantwortung von Auskunftsanfragen.

D Übermittlung ins Ausland

Der Datenschutz geniesst im internationalen Vergleich einen sehr unterschiedlichen Stellenwert. Damit die in der Schweiz und Europa generell geltenden Regeln nicht durch einen Export dieser Daten ausgehebelt werden können, gelten bezüglich der Übermittlung von Daten ins Ausland besondere

Regeln, welche der Aufrechterhaltung des in der Schweiz geltenden Schutzniveaus dienen sollen und gegebenenfalls zu beachten sind. Hier ist insbesondere das grundsätzlich weitaus tiefere Schutzniveau in den USA zu beachten. Eine Übermittlung ins Ausland erfolgt in der Praxis oftmals unbewusst z.B. bei der Verwendung elektronischer Kommunikationsmittel.

E Bearbeitung von Daten durch weitere Dienstleister (Auftragsbearbeiter) / Anpassung und Erarbeitung weiterer Dokumente

Soweit Sie für die Erbringung Ihrer Dienstleistungen mit Partnern zusammenarbeiten und diese in Ihrem Auftrag Personendaten bearbeiten, genügt es nicht, die Betroffenen darüber zu informieren. Das Datenschutzgesetz macht darüber hinaus Vorgaben über die vertraglichen Regelungen zwischen Ihnen, als Datenschutzverantwortlichem und ihren Datenbearbeitungspartnern.

Zur Umsetzung der Vorgaben der Datenschutzgesetzgebung kann es schliesslich erforderlich sein, dass weitere bereits von Ihnen verwendete Dokumente anzupassen sind. Zu denken ist hier z.B. an Arbeitsvertragsvorlagen und andere Dokumente im Rahmen eines Arbeitsverhältnisses, in denen ein zukünftiger Mitarbeitender über die Bearbeitung seiner Daten informiert werden sollte. Oder es sind neue Dokumente zu erstellen, beispielsweise interne Weisungen zum Umgang bei Auskunftsbegehren oder interne Konzepte zur sicheren Aufbewahrung und Löschung von Daten.

➔ Wir unterstützen Sie bei der Ausarbeitung transparenter Formulierungen zur Information der Betroffenen respektive adäquater Verträge mit Datenbearbeitungspartnern, sowie weiteren Dokumenten.

F. Sanktionen und Risiken

Verschiedene, im Strafgesetzbuch mit Strafe bedrohte Tatbestände können gleichzeitig einen Verstoss gegen das Datenschutzgesetz darstellen. Beispielsweise die unbefugte und heimliche Aufnahme von Gesprächen (hier nicht weiter vertieft). Eine spezifisch datenschutzrechtliche Strafnorm findet sich in Art. 179 ^{novies} StGB, welcher die unbefugte Beschaffung von besonders schützenswerten Personendaten betrifft und dies auf Antrag mit Freiheitsstrafe bis zu drei Jahren sanktioniert.

Weitere Strafbestimmungen, welche maximal eine Busse, allerdings in empfindlicher Höhe (bis zu CHF 250'000) vorsehen, finden sich im Datenschutzgesetz selbst. Dazu gehören beispielsweise die vorsätzliche Erteilung einer falschen oder unvollständigen Auskunft, das vorsätzliche Unterlassen der Information über eine Datenbeschaffung, die vorsätzliche Erteilung einer falschen Auskunft an den Eidgenössischen Datenschutzbeauftragten, die vorsätzliche Verletzung der Sorgfaltspflichten bei der Bekanntgabe von Daten ins Ausland, bei der Datenbearbeitung durch Dritte, oder die Verletzung der Mindestanforderungen an die Datensicherheit.

Schliesslich statuiert das Datenschutzgesetz eine eigentliche neue berufliche Schweigepflicht für Personen, die geheime Daten im Rahmen der Berufsausübung bearbeiten, oder auch nur von solchen im Rahmen ihrer Tätigkeit oder Ausbildung bei einer geheimhaltungspflichtigen Personengruppe erfahren. Dabei endet die Schweigepflicht nicht mit der Beendigung des Arbeitsverhältnisses der bearbeitenden Person, sondern bleibt zeitlich unbeschränkt bestehen. Es bleibt abzuwarten, wie die Praxis diese Bestimmung, welche potenziell eine enorme Tragweite hat, anwenden wird.

➔ Wir unterstützen Sie bei Risikoabschätzungen im Zusammenhang mit ihrer konkreten Tätigkeit.

RESUME
Technischer Fortschritt und globale Vernetzung vereinfachen und beschleunigen das Geschäftsleben durch die Mittel der Datenverarbeitung in jeder Hinsicht. Ein Missbrauch soll nach dem Willen des Gesetzgebers durch rechtliche Rahmenbedingungen verhindert werden, die zur Einhaltung angemessener technischer, organisatorischer und rechtlicher Massnahmen führen. Bei der Umsetzung dieser Massnahmen ist es von Vorteil, sich auf einen Partner abstützen zu können, der Sie mit entsprechender Expertise und Umsicht unterstützt, vermeidbare Reputationsschäden, nachteilige finanzielle Folgen und strafrechtliche Verantwortlichkeiten zu vermeiden.