IT & LAW CONSULTING GMBH

Digitalisierung

Rechtliche Rahmenbedingungen

KMU-Tag vom 27. Oktober 2017

mag. iur. Maria Winkler

Agenda

- **Digitalisierung unternehmerischer Abläufe**
- Cloud Services: Nutzen und Risiken
- Neue Anforderungen im Datenschutz
- Elektronische Aufbewahrung von Dokumenten
- Empfehlungen

Digitalisierung unternehmerischer Abläufe

- Mit der Digitalisierung werden unternehmerische Abläufe geändert. Dabei müssen, neben technischen und organisatorischen auch rechtliche Anforderungen beachtet werden.
- Beispiele:
  - Kann per Mobile Device ein Vertrag geschlossen werden?
  - Dürfen Kundenprofile gebildet werden? Welche Daten dürfen dazu verwendet werden?
  - Dürfen die Kundendaten in die Cloud ausgelagert werden? Wer ist verantwortlich dafür, dass die Daten geschützt werden?
  - Was muss beachtet werden, wenn die Software nicht mehr auf den eigenen Systemen installiert, sondern als «Service» bezogen wird?
  - Dürfen die Geschäftsdokumente ausschliesslich elektronisch aufbewahrt werden oder müssen weiterhin Papierdokumente archiviert werden?

Anpassung der Gesetzgebung?

- Oft sind nur die Prozesse und die verwendeten Technologien neu, nicht jedoch die rechtlichen Fragestellungen.
- Die technologische Entwicklung führte in den letzten Jahren zu einigen Gesetzesänderungen, die für KMU relevant sind.
- Beispiele:
  - Buchführung und Rechnungslegung (Art. 957 ff OR)
  - Gleichstellung der elektronischen Signatur mit der Handunterschrift (Art. 14 Abs. 2bis OR, Bundesgesetz über die elektronische Signatur, ZertES)
  - Datenschutzgesetz (DSG; zurzeit in Revision)
  - Gesetz gegen den unlauteren Wettbewerb (UWG)

Agenda

- Digitalisierung unternehmerischer Abläufe
- **Cloud Services: Nutzen und Risiken**
- Neue Anforderungen im Datenschutz
- Elektronische Aufbewahrung von Dokumenten
- Empfehlungen

Cloud Computing

- Es handelt sich (aus rechtlicher Sicht) um einen **Outsourcingvertrag**, welcher die folgenden Merkmale aufweist:
  - Die Leistungen weisen einen hohen Grad an Standardisierung auf.
  - Der Kunde hat keine Kontrolle über den aktuellen Standort seiner Daten.
  - Daten werden in der Regel (auch) im Ausland bearbeitet.
  - Die Menge der geforderten Leistung kann variieren (Skalierbarkeit).
  - Es besteht eine grosse Abhängigkeit vom Netz.
- Services, die aus der Cloud bezogen werden können, versprechen Effizienzsteigerung und Kosteneinsparungen.

Outsourcing der Datenbearbeitung

(Art 10a DSG)

- Gemäss Art. 10a DSG kann die Datenbearbeitung an einen Leistungserbringer übertragen werden, wenn
  - die Daten nur so bearbeitet werden, wie der Auftraggeber es selbst tun dürfte (**Zweckbindung**),
  - keine gesetzliche oder vertragliche **Geheimhaltungspflicht** es verbietet und
  - der Auftraggeber sich vergewissert, dass die **Datensicherheit** gewährleistet ist.
- Das outsourcende Unternehmen bleibt für die korrekte Bearbeitung seiner Daten durch den Dienstleister verantwortlich. Er muss ihn sorgfältig auswählen und kontrollieren.

Übermittlung ins Ausland (Art. 6 DSG)

- Befinden sich Rechenzentren des Cloud-Anbieters (oder seiner Subunternehmer) im Ausland, dann muss **zusätzlich** Art. 6 DSG beachtet werden.
- Die Übermittlung ins Ausland ist nur zulässig, wenn im Empfängerstaat eine (Datenschutz)Gesetzgebung herrscht, welche einen **angemessenen Schutz** gewährleistet. Der EDÖB führt eine Staatenliste, aus welcher der Stand des Datenschutzes ersichtlich ist.
- Ist dies nicht der Fall, dann muss der angemessene Schutz durch zusätzliche Garantien (Art. 6 Abs. 2 DSG) hergestellt werden – dazu zählt insbesondere der Abschluss von Verträgen mit dem Datenempfänger oder die Einwilligung der betroffenen Personen.

Kontrollrechte

- Gemäss Art. 10a Abs. 2 DSG muss sich der Auftraggeber **vergewissern**, dass die **Datensicherheit** eingehalten wird.
- Es genügt nicht, wenn der Auftraggeber die Datensicherheit nur bei Vertragserstellung beachtet – er bleibt trotz Auslagerung für die Datensicherheit verantwortlich.
- Je nach **Risikobeurteilung** sind unterschiedliche Massnahmen zu treffen:
  - Vereinbarung eines Kontrollrechts für sich und / oder für von ihm beauftragte Dritte
  - Zertifizierung des Anbieters und Einsicht in Auditberichte
  - Informationspflicht bei wichtigen Vorkommnissen
- Sind diese Massnahmen nicht umsetzbar, dann muss bei einem hohen Risiko auf das Auslagern in die Cloud verzichtet werden.

Weitere gesetzliche Anforderungen

- Da die Cloud-Dienstleistungen in der Regel **Standard-Leistungen** beinhalten, muss das Unternehmen vor dem Vertragsabschluss überprüfen, ob diese den gesetzlichen Anforderungen entsprechen.
- Es sind beispielsweise die **handels- und steuerrechtlichen Vorgaben** an die elektronische Aufbewahrung und Archivierung von Geschäftsdokumenten zu beachten.
- Beispiele:
  - Integrität der Dokumente (Art. 9 GeBüV),
  - Dauer der Aufbewahrung (in der Regel 10 Jahre ab Ende des Geschäftsjahres)
  - Zulässigkeit der Aufbewahrung im Ausland (Art. 10 Abs. 4 ElDI-V)
  - Bei einem Dienstleister im Ausland: Muss MwSt abgeliefert werden?

Weitere wichtige Vertragspunkte

- Aus der **Vereinbarung** muss klar hervorgehen, **welche Leistungen in welcher Menge und Qualität** bezogen werden.
- Die **Nutzungsrechte** müssen den Bedürfnissen des Unternehmens entsprechen.
- Die Qualität der Dienstleistungen sollte in **Service Level Agreements** nachvollziehbar und überprüfbar vereinbart werden (Konventionalstrafen).
- Die **Haftung** des Anbieters bei Vertragsverletzungen muss den unternehmerischen Risiken des Auftraggebers entsprechen.
- Sämtliche **Subunternehmer** müssen genannt werden – der Beizug weiterer Subunternehmer sollte an eine vorgängige Zustimmung des Auftraggebers gebunden werden.
- Es muss vereinbart werden, in welchen **Ländern** die Daten bearbeitet werden.

Vertragsauflösung und Folgen

- Um eine möglichst grosse **Unabhängigkeit** vom Anbieter zu bewahren, sollte vertraglich sichergestellt werden, dass ein Wechsel zu einem anderen Anbieter jederzeit möglich ist.
- Die **Kündigungsfristen** müssen den eigenen unternehmerischen Bedürfnissen entsprechen.
- Der Anbieter muss verpflichtet werden, bei Vertragsauflösung die erforderliche **Unterstützung** für die Migration der Daten und Dokumente auf die Systeme des neuen Vertragspartners zu leisten – die Kosten dieser Unterstützung sollten vertraglich vereinbart werden.
- Die Verwendung standardisierter Technologien und Schnittstellen sollte vereinbart werden (**Portabilität**).

Agenda

- Digitalisierung unternehmerischer Abläufe
- Cloud Services: Nutzen und Risiken
- **Neue Anforderungen im Datenschutz**
- Elektronische Aufbewahrung von Dokumenten
- Empfehlungen

Revision DSG

- Der Entwurf des revidierten DSG (E-DSG) sowie die Botschaft des Bundesrates wurden am **15. September 2017** veröffentlicht.
- Wann das revidierte DSG in Kraft treten wird, ist ungewiss, **frühestens jedoch im Herbst 2018**. Es wird eine **Übergangsfrist** für die Umsetzung geben.
- Die Revision des DSG bezweckt unter anderem die **Anpassung an die neuen Technologien**.
- Die neuen Vorschriften werden sich auch auf die **Bearbeitung von Kundendaten** auswirken. Im Folgenden werden einige Beispiele genannt.

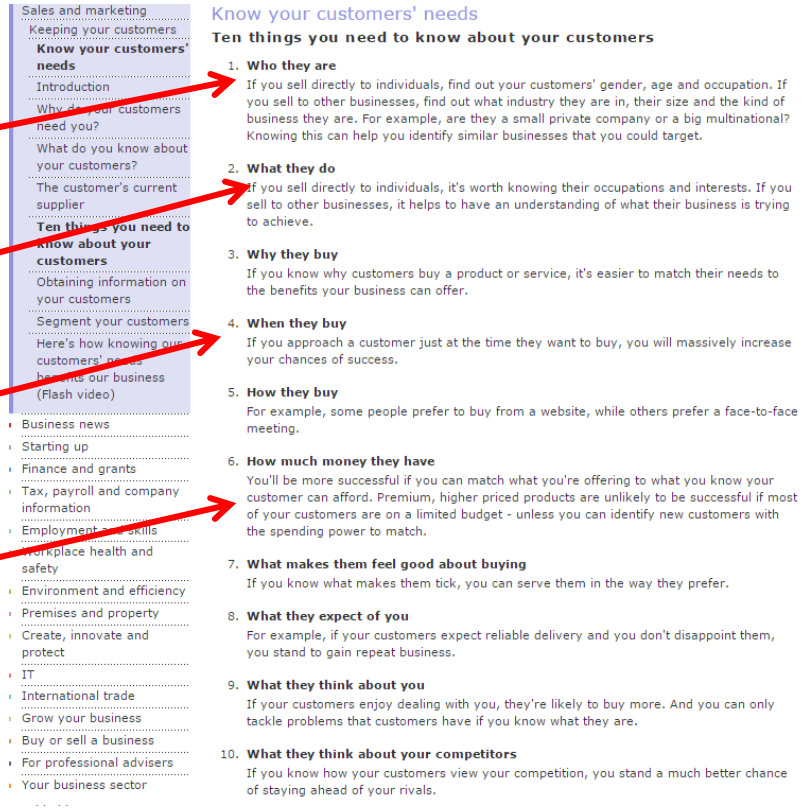
Ten things you need to know about your customers

Who they are

What they do

Why, when and how they buy

How much money they have



https://www.nibusinessinfo.co.uk/content/ten-things-you-need-know-about-your-customers

Auswertung von Kundendaten - Profiling

*Die Bewertung bestimmter Merkmale einer Person auf der Grundlage von **automatisiert bearbeiteten Personendaten**, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen. (Art. 4 lit. f E-DSG)*

- Die meisten Auswertungen, die auf der Basis von Kundenkarten gemacht werden, werden als Profiling zu qualifizieren sein.
- Folge: Ist eine **Einwilligung** erforderlich, dann muss diese ausdrücklich gegeben werden. Zudem muss vor der Einführung eine sogenannte **Datenschutz-Folgenabschätzung** durchgeführt werden.

Automatisierte Einzelentscheidung

- Wird eine Entscheidung ausschliesslich aufgrund einer automatisierten Datenbearbeitung getroffen, und hat diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person, dann hat sie ein **Informations- und Anhörungsrecht**.
- Sie muss die Möglichkeit haben, ihren Standpunkt darzulegen und sie kann verlangen, dass **die Entscheidung von einer natürlichen Person geprüft wird**.
- Beispiel: Die Bank lehnt einen Kreditantrag nur aufgrund einer Systemanfrage ab.
- **Folge**: Prozesse müssen angepasst werden.

Privacy by Design/Privacy by Default

„Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, […].“ (Art. 6 Abs. 1 E-DSG)

„Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.“ (Art. 6 Abs. 2 E-DSG)

„Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.“ (Art. 6 Abs. 3 E-DSG)

Datenschutzfreundliche Technik und Voreinstellungen

- Privacy by Design bedeutet, dass die Grundsätze des E-DSG **durch geeignete Technik** sichergestellt werden. Dazu gehören zum Beispiel:
  - rasche Pseudonymisierung oder Anonymisierung;
  - den Betroffenen werden Überwachungsmöglichkeiten zur Verfügung gestellt;
  - der Betroffene gibt die zu bearbeitenden Daten selber frei (Einwilligung durch Anklicken der freizugebenden Daten).
- Privacy by Default wird durch **datenschutzfreundliche Voreinstellungen** Genüge getan. Vorwiegend bedeutet das, dass Systeme so aufgebaut werden, dass nur jene Daten erhoben werden können, welche für die Erfüllung des Verarbeitungszwecks notwendig sind.
- **Produkte und Anwendungen**, die Daten bearbeiten oder für die Datenverarbeitung verwendet werden, sollen so **entwickelt und gestaltet** werden, dass die Verantwortlichen die datenschutzrechtlichen Grundsätze einhalten können.

Pflicht zur Meldung von Datensicherheitsverletzungen

„Der Verantwortliche meldet dem Beauftragten so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.“
(Art. 22 Abs. 1 E-DSG)

- Bei einer Verletzung der Datensicherheit handelt es sich um eine Verletzung der Sicherheit, die **ungeachtet der Absicht oder der Widerrechtlichkeit** dazu führt, dass Personendaten **verlorengehen**, **gelöscht**, **vernichtet** oder **verändert** werden oder Unbefugten **offengelegt** oder **zugänglich** gemacht werden. (Art. 4 lit. g E-DSG)
- Wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, muss auch die betroffene Person informiert werden.
- **Folge:** Ein Meldeprozess muss eingeführt werden.

Strafrechtliche Sanktionen

- Die vorsätzliche Verletzung bestimmter datenschutzrechtlicher Pflichten kann zu einer Geldstrafe von bis zu **CHF 250‘000.00** führen.
- Bestraft werden die **Mitarbeitenden.** Das Unternehmen wird in Ausnahmefällen bestraft, wenn die Busse nicht mehr als CHF 50’000.00 beträgt.
- Strafbar sind unter anderem
  - die Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 54 E-DSG);
  - die Datenbekanntgabe in ein Empfängerland unter Missachtung der Voraussetzungen des Art. 13 Abs. 1 und 2 E-DSG;
  - die Übertragung der Datenbearbeitung an einen Dritten, ohne dass dieser die Datensicherheit gewährleisten kann;
  - die Nichteinhaltung der Mindestanforderungen der Datensicherheit;
  - die Missachtung von Verfügungen des EDÖB (Art. 57 E-DSG).

Agenda

- Digitalisierung unternehmerischer Abläufe
- Cloud Services: Nutzen und Risiken
- Neue Anforderungen im Datenschutz
- **Elektronische Aufbewahrung von Dokumenten**
- Empfehlungen

Aufbewahrungspflichten

- **Geschäftsdokumente** bzw. die darin enthaltenen Informationen stellen für Unternehmen und Behörden einen bedeutenden Vermögenswert dar.
- Jedes Unternehmen muss die Dokumente aufbewahren, welche es selbst erstellt oder von Dritten erhält und die
  - sich in der **Buchhaltung** niederschlagen
  - aus **Beweisgründen** zur Geltendmachung von eigenen Ansprüchen oder zur Abwehr von Ansprüchen Dritter benötigt werden
  - aufgrund von **Spezialgesetzen** erstellt und archiviert werden müssen.

Aufbewahrungspflichtige Dokumente

Art. 958f OR

- Geschäftsbericht
- Revisionsbericht

schriftlich, unterzeichnet, **im Original** aufbewahren

- Geschäftsbücher
- Buchungsbelege

schriftlich, elektronisch oder in vergleichbarer Form aufbewahren sofern

- Gewährleistung Übereinstimmung mit den ihnen zugrunde liegenden Geschäftsfällen und
- jederzeit lesbar gemacht werden

Beweisrecht

- Das Unternehmen muss zudem alles aufbewahren, was in einem allfälligen späteren Rechtsstreit als **Beweismittel** benötigt wird (Sorgfaltspflicht) oder die es aufgrund einer gesetzlichen Verpflichtung aufbewahren muss.
- Beispiele:
  - AGB, Rechtliche Hinweise, Vertragscharakter
  - Werbematerialien, Offerten, Preislisten
  - Interne Weisungen (z.B. gegen Forderungen aus Arbeitsrecht)
  - Handbücher (z.B. gegen Forderungen aus Haftpflichtrecht)
  - Diese Dokumente werden häufig im **Intranet**, auf einer **Website** oder auch auf der eigenen **Facebook-Seite** publiziert!

Elektronische Aufbewahrung (Art. 958f OR)

- Voraussetzungen für die elektronische Aufbewahrung von **Geschäftsbüchern** und **Buchungsbelegen**:
  - **Übereinstimmung mit den zugrunde liegenden Geschäftsfällen** ist gewährleistet
  - Sie können **jederzeit lesbar** gemacht werden
- Die Voraussetzungen der Geschäftsbücherverordnung müssen beachtet werden!

Integritätssicherung bei der Archivierung

- Zur Integritätssicherung können unterschiedliche **technische und/oder organisatorische Massnahmen** wie z.B. Signaturen, unveränderbare Datenträger, Verschlüsselungen, die restriktive Erteilung von Zugriffsberechtigungen, die Aufzeichnung von Zugriffen, etc. verwendet werden.
- Die Speicherung auf veränderbaren Datenträgern ist erlaubt,
  - wenn technische Verfahren Integrität gewährleisten (z.B. digitale Signatur)
  - und der Zeitpunkt der Speicherung nachweisbar ist (Zeitstempel)
  - und die Abläufe, Verfahren und Hilfsinformationen protokolliert werden.

Verfügbarkeit und Organisation

- Die aufbewahrten Dokumente müssen innerhalb einer **angemessenen Frist** von **berechtigten Personen** eingesehen und überprüft werden können.
- Personal, Geräte und Hilfsmittel sind während der gesamten Aufbewahrungsdauer zur Verfügung zu halten!
- Die Dokumente müssen auch in Papierform vorgelegt werden können.
- Archivierte Dokumente müssen von aktiven Informationen **getrennt** oder so gekennzeichnet werden, dass eine Unterscheidung möglich ist.
- Der **Zugriff** auf die archivierten Dokumente muss geregelt werden, Zugriffe und Zutritte sind aufzuzeichnen.
- Die archivierten Dokumente müssen regelmässig auf ihre **Lesbarkeit** überprüft werden.

Verfahrensdokumentation

- Umfangreiche Dokumentationspflichten stellen sicher, dass die Geschäftsbücher, Buchungsbelege und die Geschäftskorrespondenz während der gesamten Aufbewahrungsdauer **verstanden** werden können.
- Zu dokumentieren sind beispielsweise die technische Infrastruktur, die Organisation, die Zuständigkeiten, die Arbeitsabläufe und Verfahren, die zum Verständnis notwendig sind (**Verfahrensdokumentation**).
- Die Dokumentationen sind **aktuell** zu halten und müssen gleich lang aufbewahrt werden, wie die Geschäftsbücher.

Gesetzeskonformes Scanning

- Das Einscannen von Belegen ist dann zulässig, wenn
  - die **Vollständigkeit** und **Richtigkeit** der Information gewährleistet bleibt und
  - die **Verfügbarkeit** und die **Lesbarkeit** den gesetzlichen Anforderungen weiterhin genügen.
- Die GeBüV verlangt die **Protokollierung** des Scannings (Verfahrensdokumentation).
- **Nur wenn die gesetzlichen Voraussetzungen erfüllt sind, darf der Papierbeleg nach dem Scannen vernichtet werden!**

Agenda

- Digitalisierung unternehmerischer Abläufe
- Cloud Services: Nutzen und Risiken
- Neue Anforderungen im Datenschutz
- Elektronische Aufbewahrung von Dokumenten
- **Empfehlungen**

Empfehlungen

- Mit der Digitalisierung werden unternehmerische Abläufe geändert. Dabei müssen, neben technischen und organisatorischen auch rechtliche Anforderungen beachtet werden.
- Vor dem Start eines Digitalisierungsprojekts sollten daher auch die relevanten gesetzlichen Anforderungen erhoben werden.
- Bei der Auswertung und Analyse von Kundendaten sollten insbesondere die neuen Anforderungen des revidierten DSG beachtet werden, das voraussichtlich im Herbst 2018 in Kraft treten wird.
- Sofern die erforderlichen technischen und organisatorischen Massnahmen ergriffen werden, ist das „papierlose Büro“ bereits seit einigen Jahren gesetzlich zulässig.

Danke für die Aufmerksamkeit!

mag. iur. Maria Winkler

IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug

Telefon: +41 41 711 74 08
maria.winkler@itandlaw.ch