IT & LAW CONSULTING GMBH

Endgültige Vernichtung von Daten – Risiken und rechtliche Anforderungen

Security Zone 2010

Themen

- Müssen Daten und Dokumente vernichtet werden?
  - Informationssicherheit
  - Geheimhaltungspflichten
  - Datenschutzrecht
- Wie erfolgt die gesetzeskonforme Vernichtung von Daten und Dokumenten?
- Wer trägt die Verantwortung?

IT & LAW | CONSULTING GMBH

Informationssicherheit

- Verschiedene gesetzliche Grundlagen verpflichten die Unternehmen und ihre Organe und Mitarbeitenden, die Informationen, welche im Unternehmen bearbeitet werden, zu schützen.
- Dazu zählen z.B. Normen über die kaufmännische Buchführung (**Records Management**), der **Datenschutz**, das Verbot der Verletzung von **Geschäfts- und Betriebsgeheimnissen,** die Pflicht zur Führung eines **Internen Kontrollsystems** (IKS), etc.

IT & LAW | CONSULTING GMBH

Buchführungsvorschriften

- Unternehmen, die verpflichtet sind, sich im Handelsregister eintragen zu lassen, müssen diejenigen Bücher ordnungsgemäss führen und aufbewahren, welche für die Feststellung des **Geschäftsergebnisses**, der **Vermögenslage** und der **Schuld- und Forderungsverhältnisse** erforderlich sind (Art. 957 ff. OR).
- Diese geschäftsrelevanten Dokumente müssen in der Regel für mindestens 10 Jahre archiviert werden und müssen in dieser Zeit innerhalb einer angemessenen Frist verfügbar sein.
- Die Buchführungsvorschriften verlangen nicht, dass die Daten anschliessend vernichtet werden!

Geheimhaltungsvorschriften

- Verträge mit Lieferanten oder Kunden verlangen häufig, dass Geschäfts- oder Fabrikationsgeheimnisse durch ausreichende Sicherheitsmassnahmen geschützt werden.
- Werden Dokumente, welche solche Geschäfts- oder Fabrikationsgeheimnisse enthalten vernichtet, dann muss darauf geachtet werden, dass diese nicht wiederhergestellt werden können!
- Die Verletzung von Geschäfts- und Fabrikationsgeheimnissen ist **strafbar** (Art. 162 StGB).
- Zudem droht die Geltendmachung von **Schadenersatzansprüchen**.

IT & LAW | CONSULTING GMBH

Datenschutz

Datenschutzgesetz Bund (seit 1993)

Datenbearbeitung durch

- Bundesbehörde
- Private
- Teilrevision auf 01.01.2008 in Kraft getreten

Kantonale Datenschutz-gesetzgebungen

Datenbearbeitung durch

- kantonale und
- kommunale Behörden

IT & LAW | CONSULTING GMBH

Personendaten

- **Personendaten**
  Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen
- **Besonders schützenswerte Personendaten**
  Angaben über:
  - religiöse, weltanschauliche oder politische Haltung
  - Intimsphäre, Gesundheit, ethnische Zugehörigkeit
  - Massnahmen der Sozialhilfe
  - administrative und strafrechtliche Massnahmen und Sanktionen

IT & LAW | CONSULTING GMBH

Persönlichkeitsprofile

- **Persönlichkeitsprofile** sind eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt
- Personalakten können z.B. ein Persönlichkeitsprofil darstellen

IT & LAW | CONSULTING GMBH

Bearbeiten von Personendaten

- Jeder Umgang mit Personendaten, unabhängig von den angewendeten Mitteln und Verfahren, wie z.B. das Erheben, Beschaffen, Aufzeichnen, Sammeln, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, **Vernichten** usw.
- Bei **besonders schützenswerten Personendaten** und **Persönlichkeitsprofilen** besteht eine besonders grosse Gefahr der Persönlichkeitsverletzung –ihre Bearbeitung muss daher besonders sorgfältig erfolgen

IT & LAW | CONSULTING GMBH

Verhältnismässigkeit (Art. 4 Abs. 2 DSG)

- **Verhältnismässigkeit**
  - Bearbeitung nur soweit wie für Aufgabenerfüllung notwendig und geeignet
  - Beschränkung auf das Notwendige und tatsächlich Erforderliche
  - Keine Datensammlung auf Vorrat
- Nicht mehr benötigte Daten müssen daher nach dem Grundsatz der Verhältnismässigkeit **vernichtet** oder anonymisiert/ pseudonymisiert werden, sofern keine Archivierungs- oder Aufbewahrungspflicht bestehen

IT & LAW | CONSULTING GMBH

Datensicherheit (Art. 7 DSG)

- Personendaten müssen durch **angemessene technische und organisatorische Massnahmen** gegen unbefugtes Bearbeiten, gegen die zufällige oder absichtliche Vernichtung, etc. geschützt werden.
- Die **Angemessenheit** der Massnahmen hängt von der Sensibilität der Daten ab – je grösser die Gefahr der Persönlichkeitsverletzung, umso höher ist die Sorgfaltspflicht beim Schutz der Daten.
- Diese Vorgaben sind auch bei der **Vernichtung** der Daten zu beachten!

Vernichtung von Daten und Dokumenten

- Nach Ablauf der gesetzlichen oder betrieblichen Archivierungsfrist dürfen **private Unternehmen** die Geschäftsdokumente vernichten.
- Werden **Personendaten** (z.B. Personal- oder Patientendossiers, Kundendossiers) ohne Rechtfertigungsgrund länger archiviert als gesetzlich vorgesehen, dann stellt dies eine **unverhältnismässige Datenbearbeitung** dar.
- **Öffentlich-rechtliche Institutionen** müssen die Akten dem Staats- oder Bundesarchiv anbieten - übernimmt dieses die Akten nicht, dann **müssen** diese vernichtet werden (z.B. Art. 21 Abs. 2 DSG).
- Dabei sind **datenschutzrechtliche Grundsätze** zu beachten!

Zwischenfazit

- Eine **Pflicht zur Vernichtung von Personendaten** besteht ausdrücklich im öffentlich-rechtlichen Bereich, wenn die Daten nicht vom zuständigen Archiv übernommen werden.
- **Private Unternehmen** müssen Dokumente, welche Personendaten enthalten, nach dem Grundsatz der Verhältnismässigkeit dann vernichten, wenn sie diese nicht mehr benötigen und sie diese auch nicht mehr archivieren müssen.
- Eine Pflicht zur Vernichtung von Dokumenten kann sich auch aus einer gesetzlichen oder vertraglichen **Geheimhaltungspflicht** ergeben!

IT & LAW | CONSULTING GMBH

Datenschutzkonforme Vernichtung

- Besteht eine **grosse Gefahr der Verletzung von Persönlichkeitsrechten**, oder besteht eine gesetzliche oder vertragliche **Geheimhaltungspflicht**, dann muss die Vernichtung besonders sorgfältig erfolgen.
  - Elektronische Daten müssen so gelöscht werden, dass sie nicht wieder hergestellt werden können
  - Ist dies nicht möglich, dann muss der Datenträger zerstört werden
  - Papierdokumente müssen geshreddert werden
  - Die Vernichtung durch Dritte muss kontrolliert erfolgen
- Es ist bei der anzuwendenden Sorgfalt abzustellen auf den **aktuellen Stand der Technik**!

Probleme in der Praxis

- **Wartungsverträge** mit Hardware-Lieferanten sehen oft vor, dass kaputte Datenträger zurückgesandt werden müssen – diese werden dann repariert und wieder verkauft. Es muss in diesem Fall **vertraglich sichergestellt** werden, dass die sich auf dem Datenträger befindlichen Informationen definitiv gelöscht werden – es empfiehlt sich, hier eine Konventionalstrafe zu vereinbaren, falls dagegen verstossen wird.
- **Mitarbeitende** müssen sensibilisiert werden, wie Daten und Dokumente richtig gelöscht bzw. vernichtet werden – zudem sind die Mittel zur korrekten Erfüllung dieser Pflicht zur Verfügung zu stellen.

Verantwortung

- Der VR und die GL sind zuständig für die Regelung von Verantwortlichkeiten, den Erlass von **Weisungen** und deren Kontrolle, die Bereitstellung der erforderlichen Infrastruktur sowie der personellen und finanziellen **Ressourcen**. Sie müssen zudem sicherstellen, dass die Mitarbeitenden geschult werden.
- Die **Mitarbeitenden** sind verpflichtet, Weisungen zu beachten und haben zudem eine Treuepflicht gegenüber dem Arbeitgeber. Der Arbeitgeber kann bei einer Verletzung der Weisungen Schadenersatz verlangen.
- Werden **strafrechtliche Bestimmungen** verletzt, dann ist die tatsächlich verantwortliche natürliche Person strafbar!

IT & LAW | CONSULTING GMBH

Vielen Dank für die Aufmerksamkeit!

mag. iur. Maria Winkler
IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug
041 711 74 08
maria.winkler@itandlaw.ch
www.itandlaw.ch