

Die Notwendigkeit betrieblicher Datensicherheitsmaßnahmen nach dem österreichischen Datenschutzgesetz

Das Datenschutzgesetz ist in Österreich wohl eines jener Gesetze, die am häufigsten – bewusst oder unbewusst – verletzt werden. Bisher geschah dies in den meisten Fällen ohne wesentliche Sanktionen. Dies wird sich in Zukunft jedoch aller Voraussicht nach ändern. Vor allem das Management größerer Unternehmen muss sich bewusst werden, dass darin ein nicht unerhebliches Haftungsrisiko liegt.

Das Wort Datenschutz ist heute in aller Munde. Bedingt durch die rasante Zunahme der Datenspeicherung und insbesondere des e-commerce wird Datenschutz auch für den Juristen eines der ganz großen Themen der nächsten Jahre sein.

Daten sind schon heute einer der wichtigsten „Rohstoffe“ der Wirtschaft, ihre Bedeutung wird aber in Zukunft ebenso zunehmen, wie die Gefahren, die dem einzelnen aus deren Mißbrauch drohen.

Österreich besitzt seit dem Jahr 2000 ein völlig neues Datenschutzgesetz – das sog. Datenschutzgesetz 2000 (in der Folge DSG 2000) – dieses ist naturgemäß sehr eng an die einschlägige EU-Richtlinie angelehnt. Es enthält eine Fülle von Datenschutzbestimmungen, die aber erstaunlicherweise weiten Teilen der Bevölkerung und v.a. der Unternehmen, die ja den überwiegenden Teil der Datenanwender darstellen, weitgehend unbekannt sind. Dabei spielt sicherlich mit, daß die gesetzlich vorgesehenen Sanktionen für die Verletzung der Vorschriften bis dato mangels entsprechend effizienter Verwaltungs-Strukturen kaum verhängt wurden (und wenn dies geschieht, so ohne entsprechende Publizität). Es ist aber mit Sicherheit davon auszugehen, daß diese Schonfrist für „Datensünder“ in absehbarer Zeit zu Ende gehen wird.

Diese Ausführungen beschäftigen sich nicht mit dem „Datenmißbrauch“ – daß dieser verboten ist, ist wohl allgemein bekannt (auch wenn kaum jemand im Detail weiß, was darunter konkret zu verstehen ist) – sondern mit einem anderen, bisher weitgehend unbeachteten Aspekt, der aber nicht weniger wichtig ist: **der Verpflichtung des Datenanwenders zur Ergreifung ausreichender Datensicherheitsmaßnahmen und den Konsequenzen, die eine Verletzung dieser Verpflichtung mit sich bringen kann.**

Diese Datensicherheitsmaßnahmen lassen sich in zwei große Kategorien einteilen:

- die technischen Maßnahmen und
- die Maßnahmen in Zusammenhang mit Dienstnehmern (arbeitsrechtliche Maßnahmen)

Technische Maßnahmen

Definitionen:

Bevor wir hier näher ins Detail gehen, sollten wir einige Definitionen des DSG 2000 beachten:

- **Daten:**

Angaben über Betroffene (vom Auftraggeber verschiedene natürliche oder juristische Person), deren Identität bestimmt oder bestimmbar ist.

- **Auftraggeber:**

natürliche oder juristischen Personen, die die Entscheidung getroffen haben, Daten zu verarbeiten (ermitteln, speichern, ordnen, verknüpfen, abfragen, löschen, ...) – unabhängig davon, ob sie die Verarbeitung selbst durchführen oder einen Dritten dazu heranziehen.

- **Dienstleister:**

wer Daten, die ihm zur Herstellung eines Werkes überlassen wurden, verwendet

Wer muß Datensicherheitsmaßnahmen ergreifen?

Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters sind gem. § 14 DSGVO 2016 Maßnahmen zur Gewährleistung der Datensicherheit zu treffen.

Das bedeutet, daß **jeder (!), der Daten verwendet**, vom Gesetz her verpflichtet ist, für deren Sicherheit die entsprechenden Maßnahmen zu treffen.

Welche Intensität müssen die Datensicherheitsmaßnahmen haben?

Das österreichische Datenschutzrecht geht von einem dynamischen System der Datensicherheit aus. Dies bedeutet, daß der erforderliche Umfang der Datensicherheitsmaßnahmen nicht einheitlich im Gesetz geregelt ist, sondern abhängt von

- Der Art der verwendeten Daten
- Umfang und Zweck der Verwendung
- Dem jeweiligen Stand der technischen Möglichkeiten
- Der wirtschaftlichen Vertretbarkeit

Das bedeutet also:

- Je heikler die verwendeten Daten, desto besser müssen sie geschützt werden (Gesundheitsdaten natürlicher Personen oder Kreditkarteninformationen bedürfen also eines wesentlich höheren Datenschutzniveaus als bloße Telefonnummern...)
- Die Datenschutzmaßnahmen müssen laufend der technischen Entwicklung angepaßt werden!

Wovor sind die Daten zu schützen?

Inhalt der Datensicherheitsmaßnahmen muß es sein, sicherzustellen, daß die Daten

- vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind,
- daß ihre Verwendung ordnungsgemäß erfolgt und
- daß die Daten Unbefugten nicht zugänglich sind.

Konkrete Maßnahmen

Das Gesetz enthält einen Katalog von Maßnahmen, die – soweit es das dynamische System erfordert – „insbesondere“ zu setzen sind:

- Regelung der Zugriffsberechtigung auf Daten und Programme, Schutz der Datenträger vor Einsicht und Verwendung durch Unbefugte
- Klare innerbetriebliche Regelung der Berechtigungen zum Zugriff auf die Daten
- Absicherung jedes Gerätes gegen unbefugte Inbetriebnahme
- Regelung der Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters
- Bindung der Datenverwendung an gültige Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter
- Führung und Aufbewahrung (üblicherweise 3 Jahre) entsprechender Protokoll-Dateien, um Verwendungsvorgänge auf ihre Zulässigkeit nachzuvollziehen
- Erstellung einer ausreichenden Dokumentation der getroffenen Datensicherheitsmaßnahmen, um Kontrolle und Beweissicherung zu erleichtern.

Dieser Katalog ist aber nicht abschließend formuliert – jede darüberhinausgehende Maßnahme, die nach den Umständen des Einzelfalles erforderlich ist, um ein ausreichendes Schutzniveau zu gewährleisten, ist zusätzlich zu setzen!

Arbeitsrechtliche Maßnahmen

Information der Mitarbeiter

Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die betroffenen Mitarbeiter jederzeit über die für sie geltenden Regelungen informieren können. Alle Mitarbeiter sind ausdrücklich über ihre nach dem DSG 2000 bzw nach innerbetrieblichen Datenschutzvorschriften bestehenden Pflichten zu belehren und im erforderlichen Umfang auszubilden.

Aus der Sicht des Unternehmers sollte diese Belehrung aus Beweisgründen nach Möglichkeit schriftlich – etwa bereits im Dienstvertrag – erfolgen.

Vertragliche Verpflichtung zur Wahrung des Datengeheimnisses

Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Dienstgebers übermitteln. Unter Übermittlung versteht das DSG 2000 einerseits die Weitergabe an Dritte bzw die Veröffentlichung, aber auch die Verwendung der Daten für ein anderes Aufgabengebiet des Auftraggebers als jenes, für die die Daten ursprünglich ermittelt wurden.

Auftraggeber und Dienstleister haben ihre Mitarbeiter vertraglich (!) zu verpflichten, Daten nur nach derartigen gültigen Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung ihres Dienstverhältnisses einzuhalten.

Konsequenzen mangelhafter Datensicherheit

Mangelhafte Datensicherheit im Unternehmen kann naturgemäß – wird sie von dritter Seite (etwa sog. „Hackern“) ausgenutzt oder kommt es auch nur einfach zum Datenverlust – erhebliche wirtschaftliche Folgen haben. Der Vertrauensverlust bei Kunden, deren Daten mißbraucht wurden, oder auch die Kosten der Wiederherstellung zerstörter Datensätze seien hier nur beispielsweise genannt.

Daneben sehen aber auch die einschlägigen gesetzlichen Bestimmungen rechtliche Konsequenzen für derartige Fehler vor.

Verwaltungsstrafen

Bei gröblicher Mißachtung der erforderlichen Datensicherheitsmaßnahmen kann von der zuständigen Bezirksverwaltungsbehörde eine Verwaltungsstrafe bis zu ATS 130.000 verhängt werden. Das Verwaltungsstrafverfahren wird dabei, da ja juristische Personen nicht „strafmündig“ sind, immer gegen die verantwortlichen Organe (handels- oder im Einzelfall auch gewerberechtliche Geschäftsführer, andere aufgrund der innerbetrieblichen Strukturen anordnungsbefugte Personen) geführt.

Zivilrechtliche Haftungen

Daneben besteht aber unter Umständen noch eine wirtschaftlich wesentlich größere Gefahr, die sich aus der möglichen zivilrechtlichen Haftung ergibt:

Die einschlägigen Bestimmungen des DSG 2000 stellen ein sog. Schutzgesetz i.S. des § 1311 ABGB dar. Darunter versteht man Bestimmungen, die gewissen typischen Schäden vorbeugen sollen, die sonst als „zufällig“ eingestuft würden. Wer ein solches Schutzgesetz verletzt, hat für die daraus resultierenden negativen Folgen einzustehen, sofern diese Verletzung schuldhaft erfolgt ist. Für die Annahme der Schuldhaftigkeit genügt aber bereits leichte Fahrlässigkeit.

Verfügt das Unternehmen selbst nicht über ausreichende EDV-Kompetenz, so sollte – eben um den späteren Vorwurf der Fahrlässigkeit zu vermeiden – rechtzeitig entsprechend fachkundige externe Beratung gesucht werden.

Kommt es nun zu einem Schaden, der durch die Verletzung der Datensicherheitsbestimmungen des DSG 2000 ermöglicht wurde (Datenverlust, Mißbrauch durch Dritte, etc.), so haftet der verantwortliche Auftraggeber bzw. Dienstleister für alle dritten Personen daraus resultierende Schäden. Dies kann – etwa im Falle von Kreditkartenbetrügereien aufgrund mangelhafter Datensicherheit im Bereich eines e-commerce-Unternehmens – unter Umständen ruinöse Dimensionen annehmen.

Diese Gefahr wird heute noch in vielen Unternehmen unterschätzt, alles, was „mit Computern zu tun hat“, wird vom Management „den EDV-Freaks“ überlassen. Tatsächlich sollten aber gerade Fragen der Datensicherheit „Chef-Sache“ sein!

Neben einer besonders sorgfältigen Beachtung der Datensicherheitsvorschriften sollte bei Unternehmen, die Daten verwalten, deren Mißbrauch oder Verlust hohe finanzielle Schäden verursachen kann, aber jedenfalls auch auf eine ausreichende Versicherungsdeckung für derartige Schäden geachtet werden.

Dr Georg Röhner, Rechtsanwalt in Wien

© Dr Georg Röhner, 2001