IT & LAW CONSULTING GMBH

Datenschutz aktuell

Themenblock 5

Wirksames Risikomanagement im Datenschutz

mag. iur. Maria Winkler, 18. März 2014

Agenda

- Datenschutz in Projekten
- Typische Fälle von Datenverlust und Datendiebstahl
- Strafbare Handlungen
- Zivilrechtliche Haftung
- Korrekte Entsorgung von Daten (Vernichtung)

Datenschutz in Projekten

- In Projekten, welche die Bearbeitung von Personendaten zum Gegenstand haben, sollten datenschutzrechtliche Vorgaben so früh als möglich mitberücksichtigt werden.
- Ziel ist es, die Datenbearbeitungsprozesse von Beginn an gesetzeskonform zu gestalten und so nachträgliche (teure) Anpassungen zu verhindern.

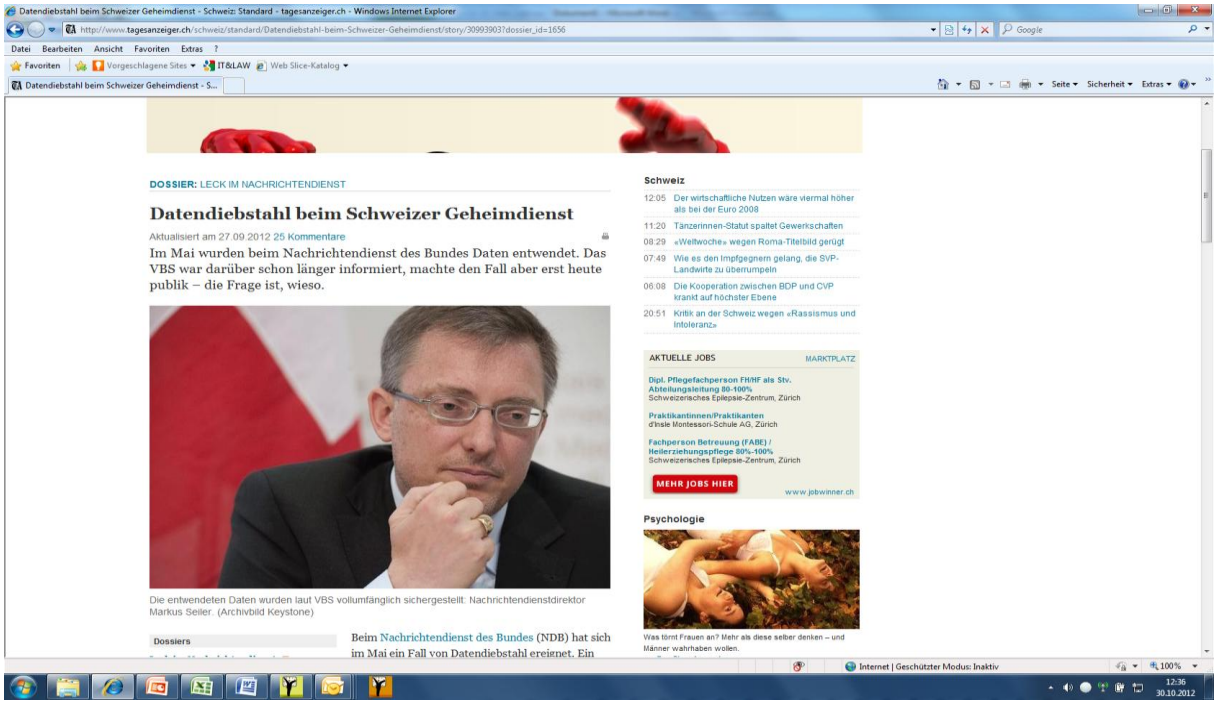
Empfehlungen

- Bereits bei der Planung sollte der betriebliche Datenschutzbeauftragte beigezogen werden (falls vorhanden).
- Der **Zweck** der geplanten Datenbearbeitung sollte möglichst genau definiert werden.
- Es gilt der Grundsatz der **Datensparsamkeit** – es sollten so wenige Daten wie nötig bearbeitet werden.
- **Tests** sollten mit anonymisierten Daten bzw. mit Testdaten durchgeführt werden.
- Die Datensicherheit muss jederzeit gewährleistet werden.

Typische Fälle von Datenverlust und Datendiebstahl (Data Leakage)

- Zahlreiche Fälle von Datenverlusten wecken das Interesse und die Sensibilität der Öffentlichkeit für die damit zusammenhängenden Fragen.
- Beispiele:
  - Wer haftet im Fall eines Datenverlusts?
  - Wer ist verantwortlich?
  - Welche Massnahmen zur Verhinderung von Datenverlusten muss man zwingend ergreifen, was ist „nice to have“?
  - Welche rechtlichen Grundlagen bestehen überhaupt?

Datendiebstahl beim Schweizer Geheimdienst



Quelle: Tagesanzeiger, http://www.tagesanzeiger.ch/schweiz/standard/Datendiebstahl-beim-Schweizer-Geheimdienst/story/30993903?dossier_id=1656

Worum geht es?

- Data Leakage erfasst Fälle des Verlusts der Vertraulichkeit, der Verfügbarkeit oder der Integrität von Daten.
- Dazu gehören beispielsweise
  - Datendiebstahl
  - Zugriff unberechtigter Dritter
  - Datenverlust durch technische Mängel, Manipulationen, etc
  - Veränderung von Daten
  - Etc.

Rechtliche Aspekte

- Im Zusammenhang mit Data Leakage geht es aus rechtlicher Sicht häufig um die folgenden Fragen und Themen:
  - Datenschutz: Was wird genau geschützt? Was verlangt das Gesetz?
  - Geschäfts- und Fabrikationsgeheimnis: Was wird geschützt? Wann liegt eine Verletzung vor?
  - Buchführungspflicht: Verlangt das Gesetz eine „nicht veränderbare“ Aufbewahrung und Archivierung?
  - Strafrechtliche Aspekte: Wann wird die Grenze zur Strafbarkeit überschritten?
  - Verantwortung: Wer haftet wofür? Welche Präventionsmassnahmen muss man ergreifen?

Strafbare Handlungen

- Das Strafgesetzbuch kennt verschiedene Normen, welche den unberechtigten Zugriff, die Veränderung oder Weitergabe von Daten unter Strafe stellen.
- Beispiele:
  - Unbefugte Datenbeschaffung (Art. 143 StGB)
  - Unbefugtes Eindringen in ein Datenverarbeitungs-System (Art. 143bis StGB)
  - Unbefugtes Beschaffen von Personendaten (Art. 179novies StGB)
  - Verletzung des Amts- oder Berufsgeheimnisses (Art. 320 ff StGB, Art. 35 DSG)
  - Verletzung des Geschäfts- oder Fabrikationsgeheimnisses (Art. 162 StGB, Art. 6 UWG, Art. 273 StGB)

Wie und gegen wen kann vorgegangen werden?

- **Strafrechtlich** (z.B. Verstoss gegen Strafgesetzbuch)
  gegen Privatperson (z.B. Angestellter), subsidiär Unternehmen
- **Zivilrechtlich** (z.B. Verstoss gegen Vertrag, Persönlichkeit, Eigentum)
  gegen Privatperson oder Unternehmen
- **Verwaltungsrechtlich** (z.B. Verstoss gegen Datenschutzvorschriften)
  gegen Unternehmen, ausnahmsweise Private
- **Aufsichtsrechtlich** (z.B. Verstoss gegen Vorschriften der FINMA)
  gegen Unternehmen

Verletzung des Fabrikations- oder Geschäftsgeheimnisses

Art. 162 StGB:

- Wer ein Fabrikations- oder Geschäftsgeheimnis, das er **infolge einer gesetzlichen oder vertraglichen Pflicht** bewahren sollte, verrät,
  wer den Verrat für sich oder einen andern ausnützt,
  wird auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

- Voraussetzung: Vertragliche oder gesetzliche Pflicht (z.B. Mitarbeiter Art. 321a OR)

Beispiel: Diebstahl einer Steuer-CD

Quelle: Handelszeitung, http://www.handelszeitung.ch/politik/julius-baer-verdacht-auf-wirtschaftsspionage

Verletzung von Fabrikations- und Geschäftsgeheimnissen

Art. 6 UWG:

- Unlauter handelt insbesondere, wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonst wie **unrechtmässig** erfahren hat, verwertet oder andern mitteilt.

Art. 23 Abs. 1 UWG:

- Wer vorsätzlich unlauteren Wettbewerb nach Artikel 3, 4, 4a, 5 oder 6 begeht, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

- Erfasst eher Externe, selten Mitarbeiter

Unbefugtes Beschaffen von Personendaten

Art. 179novies StGB:

- Wer unbefugt, **besonders schützenswerte Personendaten oder Persönlichkeitsprofile**, **die nicht frei zugänglich sind**, aus einer Datensammlung beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

- Gilt nur für „besonders schützenswerte Personendaten“ (z.B. betreffend Gesundheitszustand) oder „Persönlichkeitsprofile“
- Daten dürfen für den Täter nicht frei zugänglich sein

Unbefugte Datenbeschaffung

Art. 143 StGB:

- Wer in der **Absicht, sich oder einen andern unrechtmässig zu bereichern**, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und **gegen seinen unbefugten Zugriff besonders gesichert** sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

- Voraussetzung: Bereicherungsabsicht
- Erfasst eher Externe, selten Mitarbeiter

Unbefugtes Eindringen in ein Datenverarbeitungssystem

Art. 143 bis StGB:

- Wer auf dem Weg von Datenübertragungseinrichtungen unbefugterweise in ein **fremdes, besonders gesichertes Datenverarbeitungssystem** eindringt, wird auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
- Ebenso bestraft wird, wer Passwörter, Programme oder andere Daten, von denen er annehmen muss, dass sie zur Begehung einer strafbaren Handlung im obigen Sinne verwendet werden sollen, zugänglich macht.
- „Hackertatbestand“: Erfasst eher Externe, selten Mitarbeiter

Weitere Strafbestimmungen

- Verletzung der beruflichen Schweigepflicht (Art. 35 DSG)
- Wirtschaftlicher Nachrichtendienst bei Bekanntgabe ins Ausland (Art. 273 StGB)
- Handlungen für fremden Staat (z.B. Weitergabe von Bankkundendaten an Steuerbehörden; Art. 271 StGB)
- Fernmeldetechnisch erlangte Informationen (Art. 50 FMG)
- Urheberrechtsgesetz URG (z.B. bei unrechtmässiger Weitergabe von Software)

Zusammenfassung

- Strafe in den meisten Fällen:
  - Freiheitsstrafe **bis zu drei Jahren**
  - **Geldstrafe**
  - Voraussetzung **Antrag / Strafanzeige**

- Problematik:
  Wenn ein Mitarbeiter Täter ist, wird oft erst der Verrat und nicht eine Vorstufe hierzu bestraft. **Dann ist es zu spät!**

Vor- und Nachteile einer Strafanzeige

- Vorteile:
  - Präventiv abschreckende Wirkung gegenüber Nachahmern
  - Ruhigstellung des Täters
  - Ev. Rückgabe bzw. Einziehung von Datenträgern

- Nachteil:
  - Mögliche Veröffentlichung des Deliktes, Reputationsschaden

- Problematik:
  - Verrat nicht umkehrbar

Strafbarkeit des Unternehmens

Art. 102 StGB:

Wird in einem Unternehmen in Ausübung geschäftlicher Verrichtung … ein Verbrechen oder Vergehen begangen und kann diese Tat **wegen mangelhafter Organisation** des Unternehmens keiner bestimmten natürlichen Person zugerechnet werden, so wird das Verbrechen oder Vergehen dem Unternehmen zugerechnet. In diesem Fall wird das Unternehmen mit Busse bis zu 5 Millionen Franken bestraft.

Als Unternehmen gelten auch juristische Personen des öffentlichen Rechts und Einzelfirmen.

Zivilrechtliches Vorgehen gegen „Datendieb“

Verstoss gegen Gesetz, Vertrag, Persönlichkeit, Eigentum

- Unterlassung (ev. als vorsorgliche Massnahme)
- Rückgabe des Datenträgers
- Entlassung des Mitarbeiters
- Schadenersatz / Gewinnherausgabe: Problematik - Höhe oft nicht definierbar
- Ev. Genugtuung
- Ev. Gegendarstellung über ZGB 28

Verantwortung

- Der VR ist verantwortlich für die **Oberleitung der Gesellschaft** und für die Erteilung der nötigen Weisungen.
- Er muss die **Einhaltung von Gesetzen und Weisungen** überprüfen.
- Er kann diese Pflichten nicht delegieren und haftet für deren Verletzung (Art. 754 OR).
- Der VR ist daher zuständig für die Regelung von Verantwortlichkeiten, den Erlass von **Weisungen** und deren Kontrolle, die Bereitstellung der erforderlichen Infrastruktur sowie der personellen und finanziellen **Ressourcen**.
- Die Mitarbeitenden sind verpflichtet, die Weisungen zu beachten und haben zudem eine Treuepflicht gegenüber dem Arbeitgeber.

Massnahmen

- Infrage kommen technische und organisatorische Massnahmen wie
  - Verschlüsselung von Daten, Servern, und Kommunikationswegen
  - Restriktive Erteilung von Zugriffsberechtigungen
  - Sperren von Schnittstellen
  - Monitoring von Systemen
  - Überwachung der Mitarbeitenden
  - Personensicherheitsüberprüfungen
  - Vertragliche Geheimhaltungsvereinbarungen
  - Sicherheitskonzepte
  - Audits
  - Erlass von Weisungen und Policies, etc.
- Dabei sind die rechtlichen Rahmenbedingungen zu beachten!

Beispiel Zutrittskontrolle

- Um mit Hilfe von Zutrittskontroll-Systemen berechtigte von unberechtigten Personen unterscheiden zu können, müssen personenbezogene Daten erhoben und gespeichert werden
- Die Speicherung erfolgt auf zentralen oder dezentralen Systemkomponenten oder auch auf mobilen Datenträgern
- Werden die Daten nicht vollständig anonymisiert, müssen die **Anforderungen des Datenschutzes** beachtet werden!

Datenschuztrechtliche Anforderungen

Ausgehend vom angestrebten **Zweck** sind die folgenden Fragen zu stellen und daraus **verhältnismässige Massnahmen** abzuleiten:

- Was soll geschützt werden?
- Welche Daten werden erfasst und wie lange werden diese gespeichert?
- Welche Daten sollen von wem ausgewertet werden?
- In welcher Form soll auf unberechtigte Zutrittsversuche reagiert werden?
- Wie werden Besucher einbezogen?

Entsorgung von Daten

- Die Vernichtung geheimer oder besonders sensibler Dokumente muss **kontrolliert** erfolgen. Es muss sichergestellt sein, dass die Dokumente nach der Vernichtung **nicht wiederhergestellt** werden können.
- **Papierakten**, welche besonders schützenswerte Personendaten enthalten, oder die wegen der grossen Menge an Daten eine grosse Zahl von Personen betreffen, dürfen nicht einfach im „normalen“ Abfall entsorgt werden.
- **Elektronische Datenträger**, welche sensible Personendaten im oben genannten Sinn enthalten, müssen sicher gelöscht oder zerstört werden.
  - USB-Sticks müssen mit einem spezialisierten Programm überschrieben werden
  - Hardware muss zerstört werden oder es muss sichergestellt werden, dass die sich darauf befindlichen Daten ebenfalls überschrieben werden!

Sorgfaltspflichten

- Im Rahmen der Gewährleistung der Informationssicherheit ist das Unternehmen verpflichtet, die Daten und Dokumente mit **angemessenen Massnahmen** zu schützen – dies umfasst auch die Vernichtung von Daten!
- Die Vernichtung der Daten muss im Unternehmen **systematisch geregelt** werden und sämtliche Daten und Dokumente umfassen, unabhängig von ihrem Format.
- Werden keine oder keine ausreichenden Massnahmen getroffen, dann besteht nicht nur das Risiko von Datenschutzverletzungen sondern auch das Risiko der **Verletzung von Geheimhaltungspflichten** (z.B. Schweigepflichten im Sozialversicherungsbereich, Amtsgeheimnis, etc.).

Zusammenfassung

- Der Verlust oder der Diebstahl von Daten ist häufig die Folge von ungenügenden Massnahmen zur Gewährleistung von **Informationssicherheit** im Unternehmen.
- Die Verletzung der verschiedenen anwendbaren gesetzlichen Bestimmungen kann strafrechtliche und / oder zivilrechtliche Haftung nach sich ziehen.
- Die Unternehmensführung ist verantwortlich zur Sicherstellung der Rahmenbedingungen, die Mitarbeitenden müssen sich an die Vorgaben des Arbeitgebers halten!

IT & LAW CONSULTING GMBH

Fragen?

mag. iur. Maria Winkler
IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug
+41 41 711 74 08
maria.winkler@itandlaw.ch

Publikationen

www.itandlaw.ch