Datensicherheitsmaßnahmen nach dem DSG 2000

Dietmar Jahnel

Institut für Verfassungs- und Verwaltungsrecht, Universität Salzburg
Dietmar.Jahnel@sbg.ac.at

Zusammenfassung: *Das DSG 2000 enthält, wie schon das DSG 1978 eine Verpflichtung zur Ergreifung von Datensicherheitsmaßnahmen. Neben den bisherigen Maßnahmen, die etwa Zutritts- und Zugriffsbeschränkungen umfassen, wurde eine neue Protokollierungspflicht eingeführt. Dieser Beitrag setzt sich mit den Datensicherheitsmaßnahmen im allgemeinen und insbesondere mit den Fragen rund um die neue Protokollierungspflicht auseinander.*

Schlüsselwörter: Datenschutzrecht, Datensicherheitsmaßnahmen, Protokollierungspflicht.

1. Einleitung

Obwohl das Datenschutzrecht seit seinem Inkrafttreten am 1.1.1980 eine Verpflichtung zur Ergreifung von Datensicherheitsmaßnahmen vorsieht, ist diese Vorschrift in der Praxis wenig bekannt. Das DSG 2000 hat den Katalog der Datensicherheitsmaßnahmen des DSG 1978 übernommen und um eine Pflicht zur Protokollierung erweitert. Nicht nur wegen dieser Neuerung sollen in Folgenden die Datensicherheitsmaßnahmen nach dem DSG näher untersucht werden.
Konkret legt § 14 DSG 2000, ähnlich wie die Vorgängerbestimmungen des DSG 1978 (§ 10 für den öffentlichen Bereich, § 21 für den privaten Bereich) eine Verpflichtung für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, zur Treffung von Datensicherheitsmaßnahmen fest. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit 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.

2. Begriff der Datensicherheit

Gegenüber der Vorgängerbestimmung des § 10 DSG 1978 wurden die Zwecke der Datensicherheitsmaßnahmen erweitert. Diese sind nun nicht bloß auf die ordnungsgemäße (rechtmäßige) Datenverwendung und auf Vorkehrungen zur Geheimhaltung der Daten vor Unbefugten beschränkt, vielmehr sind nun auch Maßnahmen zur Sicherung der Daten vor Verlust oder Zerstörung umfasst. Damit nähert sich der Inhalt der Regelung den Vorstellungen der angewandten Informatik über Datensicherheitsmaßnahmen an.[1]
Zur Sicherung der ordnungsgemäßen Datenverwendung sind zunächst Maßnahmen gegen unberechtigte Speicherung und Veränderung und unrechtmäßige Weitergabe der Daten zu treffen, daneben sind aber auch Maßnahmen zur Aktualisierung, Löschung oder Anonymisierung der Daten sowie zur ordnungsgemäßen Erfüllung von Auskunfts- und Informationspflichten vorgesehen. Insbesondere soll damit die Einhaltung der in § 6 Abs 1 DSG festgelegten allgemeinen Grundsätze der Datenverwendung sicher gestellt werden.
Die Sicherung vor Verlust und Zerstörung sieht Maßnahmen gegen menschliches Handeln (zB Sabotage, Hacking, sorgfaltswidriger Umgang mit Datenträgern) vor ebenso wie Vorkehrungen gegen zufällige Ereignisse (zB Stromausfall, Wasserrohrbruch, Materialfehler und ähnliches).
Datensicherheitsmaßnahmen sind für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters zu treffen. Damit sollen alle denkbaren Untergliederungen einer Organisation erfasst werden.

3. Die Datensicherheitsmaßnahmen in Einzelnen

Durch Datensicherheitsmaßnahmen ist insbesondere sicherzustellen, dass
1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festgelegt wird;
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden werden;
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der

Datensicherheitsvorschriften bestehenden Pflichten belehrt wird;
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters geregelt wird;
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte geregelt wird;
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert wird;
7. Protokoll geführt wird, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können;
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen geführt wird, um die Kontrolle und Beweissicherung zu erleichtern.
Hinter den einzelnen Tatbeständen dieses Kataloges stehen folgende Prinzipien:
Kompetenzklarheitsprinzip (Z 1)
Auftragsprinzip (Z 2)
Belehrungspflichtprinzip (Z 3)
Zutrittsbeschränkungsprinzip (Z 4)
Zugriffsbeschränkungsprinzip (Z 5)
Betriebsbeschränkungsprinzip (Z 6)
Protokollierungs- und Dokumentationsprinzip (Z 7 und 8).

4. Risikoanalyse

§ 14 DSG verlangt aber nicht, dass bei jeder Datenanwendung ein Höchstmaß an Datensicherheitsmaßnahmen getroffen wird, sondern ermöglicht eine flexible Handhabung dieser Pflicht. Dies ergibt sich aus § 14 Abs 1 Satz 2, der eine besondere Prüfung der Verhältnismäßigkeit festlegt. Ziel ist es sicher zu stellen, dass

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

Dabei sind aber zu berücksichtigen:

- die Art der verwendeten Daten
- der Umfang und der Zweck der Verwendung
- der Stand der technischen Möglichkeiten
- die wirtschaftliche Vertretbarkeit.

Zur Beurteilung, welche Datensicherheitsmaßnahmen zu treffen sind, ist daher bei jeder Datenverwendung eine Risikoanalyse vorzunehmen. Insgesamt ist ein Schutzniveau zu gewährleisten, das den Risiken der jeweiligen Datenverwendung und der Art der zu schützenden Daten angemessen ist, wobei technische und wirtschaftliche Aspekte der Schutzmaßnahmen zu berücksichtigen sind.
Hinsichtlich der Art der Daten wurde in der bisherigen datenschutzrechtlichen Literatur folgende Skala aufgestellt, wobei die Schutzwürdigkeit und damit die Vermutung der Unzulässigkeit einer Übermittlung von oben nach unten zunehmen:[2]

- Name, Adresse, Geburtsdatum, Telefonnummer
- Informationen aus öffentlich zugänglichen Quellen; berufliche Stellung, Ausbildung
- Finanzielle Stellung, Einkommen, Bonität, finanzielle Verpflichtungen
- Freizeitgewohnheiten, Liebhabereien, Lebensgewohnheiten, Kaufgewohnheiten
- Verdachtsmomente, Vorstrafen, Intimleben, aus der Psyche stammende Daten, Familiendaten, Abnormalitäten.

Diese Skala ist nach dem DSG 2000 insofern zu modifizieren, als nunmehr die sog. „sensiblen Daten“ (nach § 4 Z 2 DSG Daten von natürlichen Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben) höchste Schutzwürdigkeit genießen. Eine Stufe darunter liegen in der Skala der Schutzwürdigkeit die „strafrechtsrelevanten“ Daten, die durch die Sonderbestimmung des § 8 Abs 4 DSG zwischen sensiblen und nichtsensiblen Daten eingestuft werden. Eine gegenüber den nichtsensiblen Daten erhöhte Schützwürdigkeit von Bonitätsdaten ergibt sich aus § 18 Abs 2 DSG, wonach bestimmt Datenanwendungen erst nach einer Vorabkontrolle durch die Datenschutzkommission aufgenommen werden dürfen. Darunter fallen neben Datenanwendungen, die sensible Daten enthalten, solche die strafrechtsrelevante Daten enthalten oder die eine Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder in Form eines Informationsverbundsystems durchgeführt werden.
Die Skala der Schutzwürdigkeit nach dem DSG 2000 lautet also:

- Zulässigerweise veröffentlichte Daten oder nur indirekt personenbezogene

Daten (keine schutzwürdigen Geheimhaltungsinteressen)
- Nichtsensible Daten
- Auskunftserteilung über die Kreditwürdigkeit, Informationsverbundsysteme
- Strafrechtlich relevante Daten
- Sensible Daten (höchste Stufe der Schutzwürdigkeit).

5. Weitere Bestimmungen

Der Wortlaut von § 14 Abs 2 DSG („Insbesondere ist, ...“) lässt erkennen, dass nach der erfolgen Abwägung zwischen Schutzbedürfnis einerseits und Schutzmöglichkeiten und wirtschaftlicher Vertretbarkeit andererseits, nicht immer alle der in Z 1 bis Z 8 genannten Maßnahmen getroffen werden müssen (ebenso die Erläuternden Bemerkungen zur Regierungsvorlage 1985 betreffend die Novellierung der Vorgängerbestimmung des § 10 DSG 1978).
Die Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, dass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können. Eine Belehrung hat nach § 14 Abs 1 Z 3 DSG ebenfalls zu erfolgen.
Der Betroffene hat grundsätzlich keinen Anspruch auf Behebung von Sicherheitsmängeln. Sicherheitsmängel können aber eine Haftung des Verantwortlichen begründen, wenn sie ursächlich zur Verletzung des Rechtes auf Geheimhaltung (§§ 31, 32 DSG) oder zu einer Schädigung des Betroffenen (§ 33) führen.[3] Weiter ist zu beachten, dass ein gröbliches Außerachtlassen der Datensicherheitsmaßnahmen eine Verwaltungsübertretung gem § 52 Abs 2 Z 4 DSG darstellt, die mit einer Verwaltungsstrafe bis zu S 130.000,-- geahndet werden kann.

6. Die Protokollierungspflicht

Insbesondere bei der Protokollierungspflicht, die durch das DSG 2000 neu eingeführt wurde, stellen sich Fragen nach Verpflichtung, Umfang und Dauer der Aufbewahrung, die im Folgenden näher untersucht werden sollen.
Die Protokollierung hat das Ziel, Datenanwendungen nachvollziehbar zu machen, um deren Rechtmäßigkeit zu prüfen und die Rechte von Betroffenen (zB Recht auf Auskunft, Richtigstellung und Löschung) zu wahren. Die Gestaltung der Protokollierung in Einzelnen, etwa die Frage, ob einzelne Zugriffe nur stichprobenweise protokolliert werden, hat sich an den in § 14 Abs 2 Z 7 DSG genannten Protokollierungszwecken zu orientieren. Hiebei ist die in Abs 1 geforderte Verhältnismäßigkeitsabwägung vorzunehmen.
Maßgeblich für die Beantwortung der Fragen im Zusammenhang mit der Protokollierungspflicht wird zunächst der letzte Satz von § 14 Abs 2 DSG sein, der folgendermaßen lautet: „Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“
Aus diesem Satz, der zahlreiche unbestimmte Gesetzesbegriffe enthält, ergibt sich, dass die Protokollierungspflicht jedenfalls nicht ohne Differenzierung für alle Arten von Datenverwendungen gilt. Bei der notwendigen Abwägung wiegt also die Schutzbedürfnis der Daten gegenüber der Berücksichtigung des Standes der Technik und den Kosten umso höher, je höher das Risiko ist, das von der konkreten Datenverwendung ausgeht. Dabei kommt es wieder auf die Art der Daten an (siehe die Skala der Schutzwürdigkeit oben unter Punkt 4). Daraus folgt, dass die Anforderungen an die Datensicherheitsmaßnahmen und damit an die Protokollierungspflicht bei einer bloßen Kundenverwaltung eines Unternehmen geringer sind als etwa bei der Speicherung von Daten über die Bonität oder bei gesundheitsbezogenen Daten.

a) Inhalt der Protokollierungspflicht

Nach § 14 Abs 2 Z 7 DSG ist (falls nach der Abwägung das Vorliegen einer Protokollierungspflicht grundsätzlich bejaht wurde) Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

b) Protokollierung von Übermittlungen

Hinsichtlich der Protokollierung von Übermittlungen sieht Abs 3 folgende Ausnahmen vor: Übermittlungen, die in der Standardverordnung (nach § 17 Abs 2 Z 6 DSG) oder in der Musterverordnung (§ 19 Abs 2 DSG) vorgesehen sind, bedürfen keiner Protokollierung. Dies sind zB im Rahmen der Standardanwendung SA022: „Kundenbetreuung und Marketing für eigene Zwecke“ Übermittlungen an Adressverlage und

Direktwerbeunternehmen sowie an die Konzernleitung bei gewerblichen Kunden Großkunden.
Das Gleiche gilt für Übermittlungen, die beim Datenverarbeitungsregister registriert wurden. Lediglich der Rest der nicht registrierten Übermittlungen (§ 17 Abs 2 Z 1 bis 5 DSG), die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, dass dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In diesen Fällen sind also allfällige Empfänger oder Empfängerkreise von Übermittlungen zu protokollieren.

c) Verwendungsbeschränkung der Protokolldateien

Protokolldaten geben nicht nur Informationen über die Rechtmäßigkeit der Verwendung von Daten, aus ihnen können meist – unmittelbar oder mittelbar – auch andere Informationen gewonnen werden. So können etwa bei Auswertung von Abfrageprotokollen eines Informationsverbundsystems Rückschlüsse über räumliche Bewegungen des abfragenden oder des abgefragten Menschen oder über sein Kaufverhalten (Kreditkartenabrechnung) gezogen werden, oder es lassen sich aus Zugriffsprotokollen für den Arbeit- oder Dienstgeber Informationen über die Einhaltung von Arbeits- oder Dienstzeiten oder die Arbeitsleistung gewinnen.
§ 14 Abs 4 DSG sieht eine Beschränkung für die Verwendung der Protokolldateien vor: Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Sie dürfen also grundsätzlich nur zur Kontrolle der Rechtmäßigkeit der Datenverwendung, also zur Prüfung, ob eine Datenverwendung nach den Bestimmungen des DSG 2000 erfolgt ist, verwendet werden. Die Rechtmäßigkeit der Verwendung betrifft auch Fragen, ob ein Dienstleister Vereinbarungen der Auftraggeber eingehalten hat und ob Mitarbeiter von Auftraggebern oder Dienstleistern nach den Weisungen der anordnungsbefugten Organe vorgegangen sind. [1]
Eine Durchbrechung der Verwendungsbeschränkung sieht das DSG 2000 nur für sicherheitspolizeiliche und strafprozessuale (kriminalpolizeiliche) Zwecke vor, jedoch auch in diesen Fällen nur zur Verhinderung von schweren Delikten (fünf Jahre übersteigende Freiheitsstrafe oder Verbrechen nach § 278a StGB [kriminelle Organisation]).

d) Aufbewahrungsfrist

Von Bedeutung ist schließlich noch § 14 Abs 5 DSG, der eine gesetzliche Aufbewahrungspflicht für Protokolldaten vorsieht. Danach sind, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.
Längere gesetzliche Aufbewahrungsfristen sehen etwa die Steuergesetze vor (7 Jahre nach § 132 BAO). Nach Satz 2 ist eine Abweichung von der Dreijahresfrist in beide Richtungen möglich.

7. Beispiel: Web-Logs und Protokollierungspflicht

Von Internet-Providern wird häufig die Frage gestellt, ob im Zusammenhang mit der Führung von Web-Logs eine Protokollierungspflicht nach dem DSG besteht.
Bei Beantwortung dieser Frage ist zunächst davon auszugehen, dass in diesem Fall die Datei, in der die Web-Logs enthalten sind, die „Datenverwendung“ darstellt. Ob das Führen von Weg-Logs überhaupt nach dem DSG bzw nach dem TKG zulässig ist, ist gesondert zu prüfen (siehe dazu [4]).
Als nächster Schritt ist eine Risikoanalyse vorzunehmen, wie sie unter Punkt 4 beschrieben wurde. Da der Inhalt von Weg-Logs das Zugriffsverhalten auf Internetseiten aufzeichnet, können prinzipiell alle Arten von Daten – und damit auch sensible Daten – enthalten sein. Eine Protokollierungspflicht wird also regelmäßig zu bejahen sein. Dies bedeutet aber nicht, dass die Web-Logs selbst zu protokollieren und aufzubewahren sind. Die Protokollierungspflicht besteht hinsichtlich des Zugriffs auf die Web-Logs und zwar insbesondere hinsichtlich der Abfragen, Änderungen und Übermittlungen der Web-Logs. Da also nur die Zugriffe auf die Web-Logs zu protokollieren sind, wird sich auch der technische und wirtschaftliche Aufwand in Grenzen halten.
Diese Protokolldatei wird in der Regel drei Jahre lang aufzubewahren sein.

[1] Drobesch/Grosinger, Das neue österreichische Datenschutzgesetz, Juridica-Verlag, Wien 2000, 165 – 169.
[2] Stadler, Wirtschaftsinformationen und Datenschutz, ÖZW 1979, 9 (13).
[3] Duschanek, Datenschutzgesetz 2000, Verlag der Wirtschaftskammer Österreich, Wien 2000, Z 6 zu § 14 DSG.
[4] Jahnel, Datenschutz im Internet. Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84.