DATENSICHERHEIT - WAS VERLANGT DAS DSG 2000?

Sowohl Auftraggeber als auch Dienstleister sind nach dem DSG 2000 zur Ergreifung von Datensicherheitsmaßnahmen verpflichtet. Sie müssen für alle ihre Organisationseinheiten Maßnahmen zur Gewährleistung der Datensicherheit treffen.

Je nach 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 ist sicherzustellen, dass

- die Daten vor zufälliger oder unrechtmäßiger Zerstörung und
- vor Verlust geschützt sind,
- dass die Datenverwendung ordnungsgemäß erfolgt und
- dass die Daten Unbefugten nicht zugänglich sind.

Unter diesen Prämissen ist daher insbesondere Folgendes geboten:

1. **Kompetenzklarheit:** Die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ist ausdrücklich festzulegen.
2. **Auftragsgebundenheit**: Die Verwendung von Daten ist an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden. Insbesondere dürfen Übermittlungen von Daten nur im Auftrag (Einzel- oder Dauerauftrag) des anordnungsbefugten Organs erfolgen.
3. **Belehrungspflicht:** Jeder Mitarbeiter ist über seine nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren. Diese Belehrung sollte aus Gründen der Dokumentation nachweislich erfolgen.
4. **Zutrittsbeschränkung**: Die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters ist zu regeln. Durch eine einschränkende Zutrittsregelung zu den Räumen des Auftraggebers oder des Dienstleisters sollen die Möglichkeiten des Missbrauches und damit das Risiko von vornherein eingeschränkt werden. Der Grad und der Umfang der Schutzmaßnahmen ist dabei etwa davon abhängig, ob es sich um die Räumlichkeiten eines Rechenzentrums oder um Bildschirmarbeitsplätze in Büroräumen handelt. (Denkbar ist zB: Festlegung von Sicherheitszonen, Absicherung der Sicherheitszonen durch ein Ausweislesesystem, closed-shop-Betrieb für das Rechenzentrum, Führung von Besucherlogbüchern, Regelung für das Datenträgerarchiv.)
5. **Zugriffsbeschränkung:** Die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte ist zu regeln. Die Regelung der Zugriffsberechtigung auf Daten und Programme stellt eine der wichtigsten Maßnahmen in einem Datensicherheitskonzept dar. Durch Maßnahmen technischer (zB Ausweisleser, Zugriffsberechtigungssystem mit Passwortschutz, sowohl funktionsbezogen als auch datenbezogen, Chipkarte),

organisatorischer (zB Zugangskontrolle, periodischer Wechsel der Passwörter) und personeller Art (zB Analyse der Protokolle über unbefugte Zugriffe durch die Revision, Verwaltung der Zugriffstabellen durch einen Systemverantwortlichen) soll erreicht werden, dass nur die zur Benutzung des IT-Systems berechtigten Personen auf Daten zugreifen können.

6. **Betriebsbeschränkung:** Die Berechtigung zum Betrieb der Datenverarbeitungsgeräte ist festzulegen und jedes Gerät ist durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern. Diese Zielsetzung kann durch Maßnahmen baulicher (zB Sicherheitsschlösser, Sicherung der Außenfester durch Gitter- oder Panzerglas), technischer (zB Schlüsselschalter an den einzelnen Geräten, automatische Protokollierung insb. unberechtigter Zugriffe, Verschlüsselungssoftware, Firewal, Viren- und Trojanerschutz), organisatorischer (zB Zugangskontrolle, closed-shop-Betrieb) und personeller Art (zB Wachdienst außerhalb der Normalarbeitszeit, Zu- und Abgangskontrollen) erreicht werden.
7. **Protokollierungspflicht:** Es ist Protokoll zu führen, damit die tatsächlich durchgeführten Verwendungsvorgänge, wie insb. Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Hinsichtlich der Übermittlungen ist zu beachten, dass in der StandardVerordnung oder in der Muster-Verordnung vorgesehene Übermittlungen keiner Protokollierung bedürfen. Nicht im Datenverarbeitungsregister registrierte Übermittlungen sind so zu protokollieren, dass die datenschutzrechtliche Auskunftspflicht erfüllt werden kann.
8. **Dokumentationspflicht:** Über alle getroffenen Datensicherheitsmaßnahmen ist eine Dokumentation zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Alle Datensicherheitsmaßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risken und der Art der zu schützenden Daten angemessen ist.

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 (Ausnahme: Verbrechensverhinderung oder -verfolgung). Mit diesem Verbot soll grundsätzlich die Verwendung der Protokoll- und Dokumentationsdaten für Zwecke der allgemeinen Dienstaufsicht und Leistungskontrolle ausgeschlossen werden.

Protokoll- und Dokumentationsdaten sind grundsätzlich drei Jahre lang aufzubewahren.

Stand: Dezember 2003