

Lutz Grammann

Datenschutz für Administratoren

St. Pius-Stift Cloppenburg
13. Oktober 2010

Erwartungen an Administratoren

- Mitwirkung bei der Gestaltung technischer Systeme
 - Datenvermeidung und Datensparsamkeit
 - Technische und organisatorische Maßnahmen
 - Meldepflicht und Verzeichnis
- Wahrung des Datengeheimnisses

§ 2a KDO Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

- Hinweise auf Risiken und Schwachstellen datenverarbeitender Systeme
- Datenschutzgerechte Einrichtung und Konfiguration der Systeme
- Vermeidung von Betriebsstörungen

§ 6 Technische und organisatorische Maßnahmen

Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Anordnung, insbesondere die in der Anlage zu dieser Anordnung genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 6 Technische und organisatorische Maßnahmen

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

- 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

§ 6 Technische und organisatorische Maßnahmen

- 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
- 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

§ 6 Technische und organisatorische Maßnahmen

- 4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
- 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

§ 6 Technische und organisatorische Maßnahmen

- 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
- 7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
- 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

§ 3a KDO Meldepflicht und Verzeichnis

(1) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, Verfahren automatisierter Verarbeitung **vor Inbetriebnahme** dem Diözesandatenschutzbeauftragten zu melden.

(3) Die Meldepflicht entfällt, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter nach § 18 a bestellt wurde oder bei ihr höchstens zehn Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind.

(4) Die Angaben nach Abs. 2 sind von der kirchlichen Stelle in einem Verzeichnis vorzuhalten. Sie macht die Angaben nach Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

Beispiel 1: Rechteverwaltung

- Einrichtung und Konfiguration einer Rechteverwaltung
- Sperrung aller Rechte, die nicht benötigt werden
- Passwortmanagement
- Verschlüsselung (z.B. „Safeguard Lan Crypt“ der Firma Utimaco)

Beispiel 2: Datensicherung

- Zentrale Datensicherung auf dem Server
- Konfiguration der Datensicherung durch Administrator
- Sichere Systeme
- Regelmäßige Überprüfung der Systeme

Beispiel 3: Datenübermittlung via Internet

- Sicherung des Übertragungsweges
- MS-Exchange Server, VPN-Tunnel
- Verschlüsselung der Daten auf dem Endgerät
- Zentrale Konfiguration der Endgeräte
- Deaktivierung unerwünschter Funktionalitäten
- Möglichkeit der Fernlöschung bei mobilen Endgeräten

Beispiel 4: Internetterminals für Patienten

- Sicheres WLAN nach dem jeweiligen Stand der Technik (z.Zt. noch WPA 2)
- Konfiguration des WLAN
- Verhinderung des Zugriffs auf Clients
- Einhaltung der Verpflichtungen aus dem TMG
 - § 14 Bestandsdaten
 - § 15 Nutzungsdaten

Hierzu: BSI: Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte

Beispiel 4: Internetterminals für Patienten

- **§ 14 Bestandsdaten**
 - Notwendig zur Begründung und inhaltlichen Ausgestaltung
 - Auskunft an Polizei/Kripo/BND/MAD auf richterliche Anordnung im Einzelfall
 - Keine Vorratsdatenspeicherung mehr! (bis auf weiteres?)
- **§ 15 Nutzungsdaten**
 - Notwendig zur Inanspruchnahme von Telemedien
 - Nutzung nach Ende der Verbindung nur für Abrechnungszwecke
 - Nutzerverhalten in der Abrechnung nur bei EVN

Beispiel 5: E-Mail

- Eindeutige Zuordnung (personalisierte E-Mail-Adresse)
- Eindeutige Trennung zwischen privaten und dienstlichen Mails
- Fernmeldegeheimnis
- Verschlüsselung für Mails mit pD (S/MIME, PGP)
- Notwendige Angaben in dienstlichen Mails (Signaturen)

§ 4 KDO Datengeheimnis

Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

- Mehr, als „nur“ Verschwiegenheit
- Umfasst alle Phasen der Datenverarbeitung
- Also auch keine unbefugte Erhebung
- Verpflichtungserklärung auch für Administratoren

Schlussbemerkung

Vielen Dank für Ihr Interesse und Ihre Geduld!

Der Diözesandatenschutzbeauftragte
Der (Erz-)Bistümer Berlin, Hamburg, Hildesheim,
Magdeburg, Osnabrück und des Offizialats Vechta
Engelbosteler Damm 72 - 30167 Hannover
Tel: 0511 - 81 93 15 - Fax: 0511 - 81 21 35
E-Mail: info@datenschutz-kirche.de
Internet: www.datenschutz-kirche.de