



Orientierungshilfe

Datenschutz bei Notarinnen und Notaren

Herausgeberin: Die Landesbeauftragte für Datenschutz
und Informationsfreiheit der
Freien Hansestadt Bremen

Bremerhaven, 15. Dezember 2009

Inhaltsverzeichnis

Einleitung	4
A. Aufbewahrung und Entsorgung von Papierakten	4
B. Elektronische Datenverarbeitung.....	4
I. PC-Nutzung – Zutritts-, Zugangs- und Zugriffssteuerung	5
II. Trennung von Datenverarbeitung Notariat/Rechtsanwaltskanzlei	6
III. Nutzung des Internets	6
IV. Per WLAN ins Internet	7
V. Datensicherung.....	7
VI. Mobile Endgeräte	8
VII. Wartung und Fernwartung	9
VIII. Entsorgung.....	11

Einleitung

Aufgrund bestehender Geheimhaltungspflichten und der Sensibilität der im Notariat zu verarbeitenden Daten, zum Beispiel in Eheverträgen oder Testamenten, sollte dem Datenschutz in diesem Bereich ein hoher Stellenwert zukommen. Im Land Bremen zugelassene Notarinnen und Notare fallen in den Anwendungsbereich des Bremischen Datenschutzgesetzes (BremDSG) und sind verpflichtet, dessen Vorschriften einzuhalten. Hierbei ist insbesondere auch zu beachten, dass nach § 7 a Absatz 1 BremDSG ein behördlicher Datenschutzbeauftragter zu bestellen ist. Dieser soll auf die Einhaltung des Bremischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz hinwirken. In Zweifelsfällen kann er sich jederzeit an die Landesbeauftragte für Datenschutz und Informationsfreiheit wenden.

Sinn dieser Orientierungshilfe ist es, Notarinnen und Notare bei einem datenschutzkonformen Umgang mit personenbezogenen Daten zu unterstützen. Hierbei wird sowohl auf die Arbeit mit traditionellen Papierakten als auch auf die elektronische Bearbeitung von Vorgängen eingegangen. Den Bewertungsmaßstab bildet § 7 Absatz 3 Satz 1 in Verbindung mit Absatz 4 BremDSG, wonach technische und organisatorische Maßnahmen durch die Notarinnen und Notare zu treffen sind, um den Schutz personenbezogener Daten zu gewährleisten.

Den Verfassern dieses Papiers ist bewusst, dass die konkrete Umsetzung der für die elektronische Bearbeitung beschriebenen Maßnahmen einem PC-Anwender ohne vertiefte Kenntnisse Probleme bereiten wird. Aufgrund der Sensibilität der bei Notarinnen und Notaren verarbeiteten Daten und der gesetzlichen Anforderungen sind die nachfolgend beschriebenen Maßnahmen jedoch unumgänglich. Mit der Orientierungshilfe soll den Notarinnen und Notaren eine Hilfe an die Hand gegeben werden, um - bei ausreichenden EDV-Kenntnissen - die aufgeführten Einstellungen selbst vorzunehmen oder bei ihren EDV-Dienstleistern auf deren Umsetzung hinzuwirken.

A. Aufbewahrung und Entsorgung von Papierakten

Trotz eines zunehmenden Einsatzes von modernen Informations- und Kommunikationstechnologien sind Papierakten in der täglichen Arbeit im Notariat derzeit noch nicht wegzudenken. Daten in Papierakten müssen gegen eine unbefugte Einsichtnahme geschützt werden. Um der Gefahr der unbefugten Einsichtnahme entgegenzutreten, sollte der Büroraum bei Nichtbenutzung verschlossen sein. Zumindest sind die Akten aber unter Verschluss zu lagern. Sollten aus Kapazitätsgründen abgeschlossene Akten in anderen Räumen (zum Beispiel Keller, Dachboden oder Archiv) gelagert werden, ist hierbei darauf zu achten, dass eine unbefugte Einsichtnahme ausgeschlossen ist. Die Lagerung muss in abschließbaren Schränken erfolgen, wenn nicht der gesamte Raum dem Zutritt durch Dritte entzogen werden kann.

Nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen sind die Akten datenschutzgerecht zu entsorgen. Hier empfiehlt sich der Einsatz eines geeigneten Schredders (mindestens Sicherheitsstufe 3 der DIN 32757 - vergleiche hierzu auch Orientierungshilfe „Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen“; herunterladen unter <http://www.datenschutz-bremen.de/recht.php>) oder bei größeren Datenmengen auch die Beauftragung eines professionellen Entsorgungsunternehmens. Bei der Auftragsvergabe sind die Anforderungen des § 9 BremDSG zu beachten.

B. Elektronische Datenverarbeitung

Es ist zu beobachten, dass für die Bearbeitung von Vorgängen zunehmend moderne Informations- und Kommunikationstechnologien eingesetzt werden. Die Nutzung von diesen Technologien stellt auf der einen Seite eine Arbeitsvereinfachung dar, birgt aber auch erhebliche Gefahren in sich. In § 7 Absatz 4 BremDSG sind Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen für eine datenschutzgerechte automatisierte Verarbeitung von personenbezogenen Daten festgelegt.

I. PC-Nutzung – Zutritts-, Zugangs- und Zugriffssteuerung

Computer, auf denen Notarinnen und Notare Daten verarbeiten, sind gegen eine unbefugte Nutzung zu schützen. Dazu ist zunächst eine effektive Zutrittsregelung zu den Räumen, in denen die Computer betrieben werden, notwendig. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren. Hierzu gehören insbesondere auch Server. Diese dürfen nicht frei zugänglich sein. Zur Gewährleistung von § 7 Abs. 4 Nr. 1 und 2 BremDSG (Zutritts- und Zugangskontrolle) sollten Server in abschließbaren Räumen oder verschließbaren Schränken stehen.

Zudem ist eine wirksame Absicherung der eingesetzten Computer selbst gegen unbefugte oder missbräuchliche Nutzung einzurichten. Die modernen Betriebssysteme wie Linux, Microsoft Windows XP oder Microsoft Windows 7 ermöglichen dies. PC mit diesen Betriebssystemen kann man nur nach vorheriger Eingabe eines Benutzernamens und eines Passwortes benutzen, wenn sie entsprechend konfiguriert sind.

Die verwendeten Passwörter müssen bestimmte Qualitätskriterien erfüllen. Die Sicherheit und Funktionalität der Zugangs- und Zugriffsrechteverwaltung des Systems ist entscheidend davon abhängig. Ebenso ist es wichtig, dass Passwörter korrekt verwendet werden. Passwörter müssen geheim gehalten werden und dürfen nur dem Benutzer persönlich bekannt sein. Sie dürfen nicht auf dem PC gespeichert werden.

Eckpunkte:

- Die Computer müssen so eingerichtet sein, dass sie erst nach Eingabe eines Benutzernamens und eines Passwortes genutzt werden können. Automatische Anmeldungen ohne Eingabe eines Passwortes dürfen nicht erfolgen.
- Jeder Nutzer erhält eine eigene, persönliche Zugangskennung (Benutzername).
- Passwörter müssen geheim gehalten werden. Sollte jemand Kenntnis des Passwortes erlangt haben, so muss dieses umgehend geändert werden.
- Passwörter müssen bestimmte Qualitätskriterien erfüllen und es ist zwingend erforderlich, dass korrekt und verantwortungsvoll mit ihnen umgegangen wird. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat entsprechende Anforderungen definiert und veröffentlicht. Unter folgendem Link sind diese Informationen im Internet abrufbar:
https://www.bsi.bund.de/cln_164/ContentBSI/grundschutz/kataloge/m/m02/m02011.html
- Zugangsdaten (Benutzernamen, Passwörter) dürfen nicht auf dem Computer gespeichert werden. Das bedeutet auch, dass besondere Funktionen von Internet-Browsern, wie „automatisches Vervollständigen von Passwörtern“ oder „automatisches Anmelden“ und so weiter, nicht genutzt werden sollten und am besten immer abgeschaltet sind.
- Für die tägliche Arbeit soll das entsprechende Benutzerkonto nur über eingeschränkte Rechte verfügen.
- Das Administratorkonto beziehungsweise das Benutzerkonten mit Administratorberechtigung sollen immer nur genutzt werden, wenn dies notwendig ist, zum Beispiel bei Installation oder Update von Software, Einstellung beziehungsweise Anpassung des Systems. Sobald die administrativen Arbeiten beendet sind, soll wieder mit einem Benutzerkonto mit eingeschränkten Rechten gearbeitet werden.

II. Trennung von Datenverarbeitung Notariat/Rechtsanwaltskanzlei

Häufig sind Notarinnen und Notare in Bremen auch Rechtsanwälte. Bei der Verwendung von Spezialsoftware für Notariate sind die Aufgaben des Notariats von denen der Rechtsanwaltskanzlei zu trennen. Das kann zum Beispiel durch eine Anpassung der Zugriffsrechte oder nur teilweise Installation der Software-Module gewährleistet werden, da dann nur auf die für die entsprechende Aufgabe erforderlichen Daten zurückgegriffen werden kann. Eine fehlende Trennung stellt einen Verstoß gegen den Zweckbindungsgrundsatz des § 12 Absatz 1 Bremischen Datenschutzgesetzes (BremDSG) sowie gegen das Trennungsgebot des § 7 Absatz 4 Nummer 8 BremDSG dar, wonach zu gewährleisten ist, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Wichtig ist es auch, dass Mitarbeiterinnen und Mitarbeitern der Notarinnen und Notare den Aufgaben entsprechende Rollen beziehungsweise Zugriffsrechte sowohl auf Betriebssystemebene als auch innerhalb eventuell eingesetzter Spezialsoftware zugewiesen werden können und dies auch umgesetzt wird. Dies entspricht § 7 Absatz 4 Nummer 3 BremDSG und ermöglicht differenzierte Schreib- und Leserechte auf Datenbestände und Anwendungen.

Eckpunkte:

- Eine Trennung zwischen der Datenverarbeitung eines Notariats zur Datenverarbeitung einer Rechtsanwaltskanzlei muss technisch gewährleistet werden.
- Den Aufgaben entsprechende Rollen und Zugriffsrechte sind zu vergeben.

III. Nutzung des Internets

Das Internet ist aus dem täglichen Leben nicht mehr wegzudenken. Auch für Notarinnen und Notare kann es ein nützliches Arbeitsmittel darstellen. IT-Systeme, die an das Internet angeschlossen sind, werden jedoch durch eine Nutzung des Internets von außen angreifbar. Notarinnen und Notare verarbeiten sensible personenbezogene Daten und müssen diese Daten gegen solche Gefahren schützen. Eine sichere Abschottung der EDV-Systeme im Notariat gegenüber externen Systemen ist erforderlich.

Der effektivste Schutz ist die strikte Trennung von Dienst-Rechnern und solchen zur Internet-Nutzung. Für die Internet-Nutzung sollten - idealerweise - nicht mit Arbeitsplatz-Rechnern oder Servern vernetzte Einzelplatz-Computer eingesetzt werden. Die dienstlichen Systeme können dann ausschließlich für die Vorgangsbearbeitung eingesetzt werden.

Werden Computer an das Internet angeschlossen, bedürfen sie einer Grundabsicherung. Entscheidende Maßnahmen sind dabei die Nutzung stets aktueller Virenscanner und idealerweise der Einsatz von Software-Firewalls, die direkt auf den Computern laufen (auch dann, wenn bereits in Einsatz befindliche DSL-Router eine Firewall eingebaut haben oder eine zentrale Hardware-Firewall betrieben wird). Über die Software-Firewall kann die Kommunikation des Rechners und der darauf laufenden Anwendungen mit anderen Geräten im Internet oder auch innerhalb des lokalen Netzwerks gesteuert und kontrolliert werden. Gerade wenn der Rechner mit dem Internet-Router (stellt die Verbindung in das Internet her) via WLAN (Wireless LAN = Funknetzwerk) verbunden ist, ist der Einsatz einer Software-Firewall dringend angezeigt. So kann, auch wenn mehrere Rechner sich einen Internetanschluss teilen, immer eine Abschottung gegen andere Geräte erreicht werden.

Das Betriebssystem und die für die Internet-Nutzung verwendeten Software-Komponenten (zum Beispiel Software-Firewall, Internet-Browser, Messenger-Software) müssen möglichst automatisiert auf dem neuesten Stand gehalten werden (automatische Updates), zumindest aber manuell in kurzen zeitlichen Abständen überprüft und gegebenenfalls angepasst werden.

Eckpunkte:

- Möglichst Dienst-Rechner nicht zur Internet-Nutzung einsetzen.
- Effektive Absicherung des genutzten Computer gegen Gefahren aus dem Internet: automatisch aktualisierte Virens Scanner, Einrichtung einer Software-Firewall, automatisiertes Einspielen sicherheitsrelevanter Betriebssystem-Patches.

IV. Per WLAN ins Internet

Der Einsatz von WLAN ist für die Internetnutzung sehr praktisch, da keine herkömmlichen Datenleitungen erforderlich sind. Die Nutzung von WLAN birgt jedoch besondere Gefahren in sich. Funkverbindungen lassen sich relativ leicht „abhören“. Ein Funknetz ist nicht allein auf die heimische Wohnung, das Bürogebäude oder auch nur einen bestimmten Radius um den WLAN-Router beschränkt. Zwar kann es möglich sein, dass aufgrund der Bauweise (verwendete Materialien und so weiter) eines Gebäudes nicht überall darin WLAN genutzt werden kann, von der Straße oder aus dem Nachbargebäude aber ein ungestörter und glasklarer Empfang der Funkverbindung möglich ist. Wo das WLAN empfangen werden kann, lässt sich nicht voraussagen. Daher ist es unbedingt notwendig, durch den Einsatz geeigneter starker Authentisierungs- und Verschlüsselungsmethoden die per Funk übertragenen Daten gegen unbefugte Kenntnisnahme oder Manipulation abzusichern. Dabei ist der aktuellste Stand der Technik einzusetzen. Verschlüsselungsverfahren aus den Anfangszeiten der WLAN-Technologie wie WEP sind nicht ausreichend sicher und können nach neuesten Erkenntnissen in Zeiten unter einer Minute geknackt werden. Dazu bedarf es kaum besonderer Kenntnisse: Entsprechende Softwaretools gibt es kostenlos und frei verfügbar im Internet.

Eckpunkte:

- WLAN-Einsatz birgt besondere Gefahren, insbesondere die Möglichkeit des unbemerkten „Mithörens“ der Datenübertragungen per Funk oder die unbefugte Nutzung von Funknetz und die daran angeschlossenen Komponenten oder Netze (zum Beispiel Internet).
- Eine geeignete, jeweils dem aktuellen Stand der Technik entsprechende Verschlüsselungsmethode und deren geeignete Konfiguration (keine Standardpasswörter und so weiter) sind notwendig, um unbefugtes Abhören oder unbefugte Nutzung auszuschließen.
- Genau wie bei der drahtgebundenen Vernetzung ist bei der Vernetzung mittels WLAN eine effektive Abschottung der Endgeräte (mit Virens Scanner, Firewall, ...) notwendig.
- Weiterführende Informationen sind in der Orientierungshilfe (OH) „Datenschutz in drahtlosen Netzen“, im Internet unter <http://www.datenschutz-bremen.de/technik.php> zu finden.

V. Datensicherung

Personenbezogene Daten, die elektronisch verarbeitet werden, müssen regelmäßig gesichert werden. Dies ergibt sich aus § 7 Absatz 4 Nummer 7 BremDSG (sog. Verfügbarkeitskontrolle). Die Daten müssen gegen zufällige Zerstörung oder Verlust (beispielsweise durch Diebstahl des Computer, Hardwareschäden oder Naturgewalten wie Brände) geschützt sein. Das lässt sich nur über eine geeignete Datensicherung erreichen. Wichtig ist eine regelmäßige Sicherung in kurzen zeitlichen Abständen, damit möglichst immer der aktuelle Datenbestand in den Datensicherungen enthalten ist. Nach Möglichkeit sollte die Datensicherung auf wechselnden Medien (Festplatten, Magnetbänder, CDs bzw. DVDs und so weiter) so erfolgen, dass täglich die Änderungen erfasst werden („inkrementelle Datensicherung“) und einmal wöchentlich eine Komplettsicherung der gesamten Anwendung (auch im Zusammenhang mit der Komplettsicherung des Systems möglich) inklusive Datenbestand erfolgt.

Die Datensicherung sollte möglichst mittels geeigneter Werkzeuge automatisiert durchgeführt werden. Dadurch wird - die richtige Einstellung des Werkzeugs vorausgesetzt - gewährleistet, dass die Integrität der Daten ständig überprüft und gewährleistet ist und die Datensicherung vollständig erfolgt. Bei manuell kopierten Datenbeständen auf andere Datenträger können (unbemerkt) menschliche Fehler zu totalem Verlust der Daten, Unvollständigkeit oder Verlust der Integrität der Daten führen.

Die Sicherungsmedien sind räumlich getrennt von den EDV-Anlagen zu lagern. Der räumliche Abstand sollte möglichst groß sein. Ideal wäre eine externe Lagerung der Datenbestände an einem sicheren Ort (zum Beispiel Bankschließfach).

Bei der Entsorgung von Sicherungsmedien sind besondere Anforderungen zu beachten. Dabei ist es unerheblich, ob diese noch voll funktionstüchtig oder auch mit Standardmitteln nicht mehr lesbar sind. Weitere Erläuterungen dazu sind im Abschnitt „Entsorgung“ am Ende dieses Papiers zu finden.

Eckpunkte:

- Eine regelmäßige Datensicherung ist notwendig; idealerweise Sicherung der Änderungen täglich und der gesamte Datenbestand einmal wöchentlich auf wechselnden Sicherungsmedien.
- Datensicherungen sollten automatisiert mit speziellen Sicherungswerkzeugen erfolgen, um Integrität und Vollständigkeit der Datensicherung zu gewährleisten.
- Die Protokolle der Datensicherung sollten regelmäßig geprüft werden, um Fehler zu erkennen und zu beseitigen (zum Beispiel defektes Sicherungsmedium).
- Regelmäßig sollte überprüft werden, ob die Daten aus den Datensicherungen wiederherstellbar sind.
- Die Sicherungsmedien sollten räumlich getrennt von den für die tägliche Arbeit genutzten EDV-Systemen gelagert werden.
- Bei der Entsorgung von Sicherungsmedien, egal ob funktionstüchtig oder defekt, sind besondere Randbedingungen zu beachten (siehe Entsorgung).

VI. Mobile Endgeräte

Durch die Leistungsfähigkeit mobiler Endgeräte wie Notebooks oder PDA (Personal Digital Assistant) ist es problemlos möglich, komplette Datenbestände mit sich herumzutragen und Daten bei Außenterminen zu verarbeiten. Dies birgt für den Fall, dass das Endgerät abhanden kommt (Verlieren, Vergessen, Diebstahl) besondere Gefahren in sich. Unbefugte könnten auf die Daten des Endgeräts zugreifen, wenn keine ausreichenden Sicherungsmaßnahmen getroffen wurden. Zunächst gelten die oben bereits getätigten Aussagen zu Zugriffssicherung, Internet-Nutzung und Datensicherung. Darüber hinaus ist es bei mobilen Endgeräten aber dringend erforderlich, weitere Sicherungsmaßnahmen zu ergreifen.

Die Geräte sollten nur dann genutzt werden können, wenn sie zu Beginn des Startvorgangs nach dem Einschalten erst hochfahren („booten“), wenn (bei Notebooks) vorher ein Bootpasswort eingegeben wurde. Die im Gerät eingebauten Datenträger sind zu verschlüsseln. Dann können sie nicht ohne Kenntnis des entsprechenden Schlüssels, zum Beispiel durch Umbauen in andere Computer, ausgelesen werden. Je nach eingesetzter Verschlüsselungslösung kann das Bootpasswort gleichzeitig das Passwort zur Ver- beziehungsweise Entschlüsselung des Datenträgers sein. Das bedeutet aber nicht, dass eine automatisierte Anmeldung des Benutzers nach dem Hochfahren des Betriebssystems konfiguriert werden darf. Auch auf mobilen Endgeräten müssen verschiedene Benutzerrollen abgebildet werden: normaler Benutzer, Administrator(en), Internetnutzer und so weiter. Um die Auswahl des richtigen Kontos zu ermöglichen, muss eine Auswahlmöglichkeit vor der Anmeldung am Betriebssystem vorhanden sein.

Mobile Endgeräte sind mit Einrichtungen für den Datenaustausch (zum Beispiel WLAN, Bluetooth, Kommunikation über die Infrarotschnittstelle) mit anderen DV-Systemen ausgestattet. Diese müssen

richtig konfiguriert werden, um nur gewollten Datenaustausch zu ermöglichen und ungewollten Datenverkehr zu unterbinden. Dazu zählt auch die permanente Deaktivierung einzelner Komponenten, wenn sie nicht eingesetzt werden sollen. Komponenten, die zur Kommunikation genutzt werden sollen, sollten nach Möglichkeit nur dann eingeschaltet werden, wenn diese auch benötigt werden. Nach abgeschlossenem Datenaustausch können die Komponenten wieder abgeschaltet werden. Dadurch werden unerwünschte und unbefugte Verbindungen beziehungsweise Verbindungsversuche unterbunden.

Eckpunkte:

- Die Nutzung mobiler Endgeräte soll nur nach Eingabe eines Bootpasswortes zum Hochfahren des Systems möglich sein.
- Die zentralen Datenträger sind zu verschlüsseln.
- Keine automatisierte Benutzeranmeldung: Benutzername und Passwort müssen nach dem Hochfahren des Systems zur Auswahl des Benutzerkontos mit den für die folgenden Tätigkeiten notwendigen Berechtigungen eingegeben werden.
- Kommunikationskomponenten sind permanent abzuschalten, wenn sie nicht genutzt werden, und sollten möglichst nur für die Zeiträume aktiviert sein, in denen sie auch genutzt werden. Nach der Nutzung sollten sie wieder abgeschaltet werden.
- Die Kommunikation mit anderen Endgeräten ist dem jeweils aktuellen Stand der Technik anzupassen. Je nach verwendetem Verfahren zum Datenaustausch (WLAN, Bluetooth, Kommunikation über die Infrarotschnittstelle) sind unterschiedliche Maßnahmen der Absicherung notwendig beziehungsweise möglich.
- Auch auf mobilen Endgeräten muss eine funktionsfähige Datensicherung durchgeführt werden.

VII. Wartung und Fernwartung

Hard- und Software werden in ihren Einsatzmöglichkeiten und Vernetzungsoptionen immer komplexer. Eine vollständige, sachgerechte Konfiguration und ein ebensolcher Betrieb von DV-Anlagen ist zur Gewährleistung des Schutzes für die mit den Komponenten verarbeiteten Daten zwingend erforderlich. Oft ist - nicht nur in Spezialfragen, sondern auch bei der Konfiguration für den alltäglichen Einsatz - Unterstützung notwendig. In größeren Organisationen kann dies durch zentrale Stellen mit entsprechendem Fachwissen (EDV-Abteilung, Administration und so weiter) geleistet werden.

In kleineren Notariaten oder gar bei Einzelpersonen ist es in der Regel nicht möglich, das entsprechende aktuelle Know-how selbst vorzuhalten. Daher wird manchmal auch auf Hilfe aus der Familie oder Bekanntenkreis zurückgegriffen. Bei dieser Hilfe (EDV-Support) handelt es sich um eine Datenverarbeitung im Sinne von § 9 BremDSG. Sie ist damit einer professionellen Betreuung durch ein entsprechendes Unternehmen gleichgestellt. Es ist dabei unerheblich, ob der EDV-Support per Fernwartung, zum Beispiel über das Internet, oder direkt vor Ort geschieht. Gemäß § 9 BremDSG ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Es muss ein schriftlicher Auftrag erteilt werden, in welchem die zu treffenden technischen und organisatorischen Maßnahmen festgelegt werden. Die beauftragte Person ist auf ihre Verschwiegenheit zu verpflichten.

Für Wartung und Fernwartung sind verschiedene technische und organisatorische Maßnahmen zu ergreifen, um eine datenschutzkonforme Durchführung zu gewährleisten. Insbesondere sind die folgenden Punkte zu beachten.

1. Häufigkeit und Transparenz:

Es ist sicherzustellen, dass eine Fernwartung nur im Einzelfall, mit Einverständnis des Auftraggebers und unter Aufsicht erfolgen kann. Hierzu ist ein Verfahren zur Einleitung einer Fernwartung (Benachrichtigung, Freischaltung durch den Auftraggeber = Einwilligung) zu vereinbaren. Der Wartungsvorgang muss durch den Auftraggeber jederzeit abgebrochen werden können. Der Umstand, dass von außen auf einen PC oder ein System zu administrativen Zwecken zugegriffen wird beziehungsweise werden soll, muss für die betroffenen Benutzer dieser Systeme transparent, das heißt erkennbar sein, idealerweise für die gesamte Dauer der Fernwartung. So ist für die Fernwartung eine Lösung zu wählen, bei welcher der Auftraggeber direkt am Bildschirm einen Hinweis erhält und durch Mausklick der Fernwartung zustimmen muss beziehungsweise diese ablehnen kann. Dies gilt insbesondere für Situationen, bei denen der Bildschirminhalt des Nutzers dem Fernwartenden zur Kenntnis gelangen kann. Eine Fernwartung ohne Einwilligung darf nicht möglich sein.

Gleiches gilt für die Wartung der EDV-Geräte vor Ort. Das System sollte nur dann zugänglich sein beziehungsweise zugänglich gemacht werden, wenn der Betroffene auch vor Ort ist und die Wartungsarbeiten überwachen kann.

2. Kontrolle:

Es muss kontrollierbar sein, welche Arbeiten im Rahmen von Wartung und Fernwartung durchgeführt werden, insbesondere welche Zugriffe auf personenbezogene Daten erfolgen. Dies sollte durch Beobachtung des kompletten Wartungsvorgangs durch den Betroffenen geschehen.

3. Protokollierung (Fernwartung):

Um in Zweifelsfällen eine Revision zu ermöglichen, sind die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art der Fernwartungszugriffe) in entsprechenden Protokolldateien festzuhalten und, soweit sie nicht erforderlich sind, zeitnah zu löschen.

4. Steuerung der Zugriffsmöglichkeit (Fernwartung):

Die Fernwartungsarbeiten sind idealerweise unter einer separaten, über Identifikations- und Authentisierungsmechanismen geschützten Benutzererkennung durchzuführen; hierbei ist auch der Kreis des autorisierten Wartungspersonals eng festzulegen. Solange Fernwartungszugriffe nicht erforderlich sind, sollte die Benutzererkennung deaktiviert sein. Die Zugriffsmöglichkeiten sind auf das für die Durchführung der Wartungsarbeiten erforderliche Maß zu beschränken, insbesondere gilt dies für Systemverwalterprivilegien und den Zugriff auf personenbezogene Daten.

5. Fernwartung über Wählverbindungen:

Soweit die Fernwartung über Wählleitungsanschlüsse erfolgt, muss der endgültige Verbindungsaufbau stets durch den Auftraggeber erfolgen. In Betracht kommt hier beispielsweise der automatische Rückruf über eine fest vorgegebene Nummer der Fernwartungsstelle. Diese Konfigurationsdaten sind vor unzulässigen Veränderungen zu schützen. Da die Wählleitungsanschlüsse im Rahmen der Fernwartung nur in bestimmten Fällen benötigt werden, sollte in der übrigen Zeit der Anschluss physikalisch von der Datenverarbeitungsanlage getrennt sein, um unzulässige Zugriffsversuche auszuschließen.

6. Software-Updates:

Die Übernahme neuer Programmversionen sollte grundsätzlich nicht im Rahmen der Fernwartung erfolgen. Soweit im Einzelfall unvermeidlich, ist die Übernahme zu dokumentieren und die Integrität der übernommenen Software und Daten durch geeignete Maßnahmen sicherzustellen.

7. Vertragsgestaltung:

Der bei einer „Fernwartung im Auftrag“ zugrunde liegende Wartungsvertrag sollte Regelungen hinsichtlich Art und Umfang zulässiger Wartungsarbeiten, über die Weitergabe von im Rahmen der Wartung offenbarten personenbezogenen Daten sowie die Verpflichtung zur Beachtung der für den Auftraggeber geltenden datenschutzrechtlichen Bestimmungen enthalten.

Eckpunkte:

- EDV-Support durch Dritte (auch Familienmitglieder, Freunde und so weiter) ist Datenverarbeitung im Auftrag im Sinne des § 9 BremDSG und bedarf vertraglicher Regelung.
- Personen oder Dienstleister, die den EDV-Support leisten, sind auf das Datengeheimnis zu verpflichten.
- Fernwartung nur als Einzelfall, mit Einverständnis und unter Aufsicht.
- Wenn eine Fernwartung erforderlich ist, sollte im Vorfeld ein Konzept zur Fernwartung erstellt werden.
- Kontrolle bzw. Überwachung der durchgeführten Arbeiten, insbesondere des Zugriffs auf personenbezogene Daten.
- Wartung und Fernwartung nur im Beisein des Auftraggebers.
- Protokollierung der Fernwartungsaktivitäten.
- Zugriffsmöglichkeit zur Fernwartung bei Nicht-Nutzung deaktivieren.
- Software-Updates möglichst nicht per Fernwartung.

VIII. Entsorgung

Die Entsorgung von Altgeräten oder nicht mehr benutzten oder benutzbaren Datenträgern ist ein aus Sicht des Datenschutzes leider sehr oft vernachlässigtes Thema. Die Löschung und dabei insbesondere die Vernichtung des Datenträgers wird vielfach nicht als Phase der Datenverarbeitung erkannt (§ 2 Absatz 2 Nummer 6 BremDSG). Bei der elektronischen Datenverarbeitung gestaltet sich die Entsorgung in vielen Fällen schwieriger als die Entsorgung von Daten in Papierakten. Die durchzuführenden Maßnahmen müssen jeweils den Schutzbedarf der zu löschenden Daten berücksichtigen sowie Aufwand und Kosten für eine mögliche Datenwiederherstellung.

Soweit personenbezogene Daten, die auf magnetischen Datenträgern wie Magnetbändern, Magnetbandkassetten, Disketten, Fest- oder Wechselplatten oder USB-Sticks gespeichert sind, gelöscht werden sollen, ohne dass der Datenträger vernichtet wird, empfiehlt es sich nicht, die Daten mit der Lösch- oder Formatierungsfunktion des Betriebssystems zu löschen, da beim Löschen mit der Betriebssystemfunktion die auf dem Datenträger gespeicherten Daten nicht wirklich gelöscht werden, sondern meistens lediglich im Inhaltsverzeichnis des Datenträgers gelöscht und der zugehörige Datenbereich als frei markiert werden. Die Daten selbst sind in diesen Bereichen jedoch noch solange unversehrt vorhanden, bis sie - eher zufällig und meist auch nicht vollständig - mit neuen Daten überschrieben werden. Solange die Daten nicht überschrieben sind, lassen sie sich mit frei im Internet verfügbaren Softwarewerkzeugen problemlos wieder herstellen.

Daten auf intakten magnetischen Datenträgern können durch das ein- oder mehrmalige komplette Überschreiben mit Zufallszahlen gelöscht werden. Dazu sind geeignete Softwarewerkzeuge verfügbar. Das einmalige komplette Überschreiben mit Zufallszahlen soll beim Löschen von Daten jeder Art praktiziert werden. Diese Form der Wiederaufbereitung sichert die weitere Verwendbarkeit des entsprechenden Datenträgers. Unter Umständen reicht das beschriebene einmalige Überschreiben nicht aus. Weitere Informationen zum Löschen magnetischer Datenträger bietet die Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, im Internet zu finden unter http://www.datenschutz-bremen.de/pdf/oh_sicheres_loeschen.pdf.

Optische Datenträger wie CD oder DVD können in der Regel nicht überschrieben oder durch magnetische Durchflutung zerstört werden. Die Daten sind für Spezialisten selbst dann noch rekonstruierbar, wenn zum Beispiel eine CD zerbrochen oder zerstückelt worden ist. In Abhängigkeit der

dort gespeicherten Daten sind aber trotzdem geeignete Maßnahmen für eine datenschutzgerechte Vernichtung und Entsorgung der entsprechenden Datenträger zu treffen.

Besonders problematisch ist die Entsorgung von Altgeräten. Dabei wird oft übersehen, dass die personenbezogenen Daten auf den Geräten ebenfalls endgültig gelöscht werden müssen, beispielsweise mit den oben beschriebenen Methoden.

Heikel sind auch Reparaturen oder der Austausch von Systemkomponenten, insbesondere wenn die Geräte zur Reparatur eingeschickt werden müssen und nicht vor Ort beim Eigentümer repariert werden. Während dieser Zeit kann nicht sichergestellt werden, dass Unbefugte Einblick in die auf dem System gespeicherten Daten nehmen. Daher empfiehlt es sich immer, personenbezogene Daten in verschlüsselten Bereichen von Datenträgern abzulegen, auf die auch mit Administratorberechtigung, aber ohne Kenntnis des Schlüssels nicht zugegriffen werden kann. In vielen Fällen könnten auch die Festplatten vor der Übergabe an den Reparaturbetrieb ausgebaut werden, um so eine unbefugte Kenntnisnahme zu verhindern. Schwierig wird es, wenn eine Festplatte innerhalb der Garantie ausgetauscht werden muss, etwa weil sie nicht mehr funktioniert. Da oftmals nicht transparent ist, was mit den defekten Festplatten und den darauf gespeicherten Daten nach deren Austausch passiert, muss im Zweifelsfall auf die Garantie verzichtet und die Festplatte datenschutzgerecht entsorgt werden.

Eckpunkte:

- Datenträger (auch Sicherungsmedien) mit personenbezogenen Daten müssen datenschutzgerecht entsorgt werden.
- Integrale Funktionen des Betriebssystems zum Löschen von Dateien reichen meist nicht aus, um Daten irreversibel zu löschen.
- Daten, die in Altgeräten gespeichert sind, müssen irreversibel gelöscht werden. Insbesondere deren Festplatten müssen vor Abgabe oder Entsorgung mit geeigneten Methoden gelöscht werden, aber auch die Speicher von PDA oder ähnlichen Geräten.
- Im Garantiefall möglichst die Festplatte ausbauen oder von Beginn an Daten nur in verschlüsselten Bereichen der Festplatte abspeichern. In besonderen Fällen kann es erforderlich sein, auf die Garantie zu verzichten.
- Löschen magnetischer Datenträger:
Im Internet sind unter den folgenden Links weitere Informationen zu finden:
http://www.datenschutz-bremen.de/pdf/oh_sicheres_loeschen.pdf
http://www.datenschutz-bremen.de/pdf/sicheres_loeschen.pdf
- Zum Thema Löschung von Daten und Datenträgervernichtung gibt es ebenfalls im Internet eine Orientierungshilfe mit weiterführenden Informationen:
<http://www.datenschutz-bremen.de/pdf/datenloeschung.pdf>

Bei weiteren Fragen wenden Sie sich gerne an:

**Die Landesbeauftragte für Datenschutz
und Informationsfreiheit
der Freien Hansestadt Bremen**

Anschrift

Arndtstraße 1
27570 Bremerhaven

Postanschrift

Postfach 10 03 80
27503 Bremerhaven

Tel.: (0471) 596-2010 oder
(0421) 361-2010
Fax: (0421) 496-18495

E-Mail: office@datenschutz.bremen.de
Internet-Adresse: www.datenschutz.bremen.de