Mitteilung

Richtlinie zur Arbeit mit transportablen Datenverarbeitungsgeräten und Datenträgern in den Dienststellen der Ev.-Luth. Landeskirche Sachsens

Vom 6. April 1995 (ABl. 1995 S. A 68)

Inhaltsübersicht *

1. Allgemeines

Durch den Einsatz transportabler Datenverarbeitungsgeräte und Datenträger entstehen vielfache Gefahren. Sie bestehen einerseits im Einschleppen von Computerviren in festinstallierte Standgeräte und lokale Netze, andererseits im erhöhten Diebstahlrisiko. Diese Richtlinie regelt daher den Umgang und die Arbeit mit derartigen Geräten und Datenträgern. Soweit es erforderlich ist, können im Einzelfall ergänzende Hausanweisungen in den Dienststellen erlassen werden.

* nichtamtlich

2. Begriffsbestimmungen

a) Transportable Datenverarbeitungsgeräte

Laptops, Note-Books, Pen-Pads, Pocket-Organizer, Drucker u. a.

b) Transportable Datenträger

Disketten, Wechselplatten, externe Festplatten, Data-Cardriges, Magnetbänder, Magnetkarten und künftige transportable Datenträger.

c) Fremd-Datenträger

Datenträger aus anderen Dienststellen der Landeskirche oder aus außerkirchlichen Stellen.

d) Gefährdung

Eine Gefährdung liegt vor, wenn eine Veränderung, Verfälschung oder der Verlust wichtiger Daten oder gar die Zerstörung der Gerätetechnik, der Datenträger und der dazugehörigen Software droht.

e) Boot-Lock Paßwort

Dieses Paßwort verhindert ein unbefugtes Starten des Betriebsystems nach erfolgtem Einschalten des Rechners.

f) „booten“

Starten des Betriebsystems über eine Diskette.

3. Einsatz transportabler Datenverarbeitungsgeräte und Datenträger

Transportable Datenverarbeitungsgeräte und Datenträger dürfen nur dort eingesetzt werden, wo die Verfügbarkeit von Daten, Testprogrammen, Diagnosehilfen etc. dies unbedingt erforderlich machen. Ein Einsatz solcher Geräte aus Gründen der Platzersparnis ist nicht zulässig, da ein ergonomisches Arbeiten mit diesen Geräten nicht möglich ist. Nachfolgend werden praktische

Hinweise zum Umgang mit transportablen Datenverarbeitungsgeräten und Datenträgern gegeben.

3.1. Organisatorische Maßnahmen:

1. Transportable Datenverarbeitungsgeräte und Datenträger dürfen niemals unbeaufsichtigt in öffentlichen Verkehrsmitteln oder privaten KFZ belassen werden.
2. Sie sind nach Dienstschluß verschlossen aufzubewahren.
3. Ein Einsatz privater Geräte ist nur im Ausnahmefall und auf Grund einer schriftlichen Genehmigung der Dienststellenleitung zulässig. Bei der Benutzung privater Geräte ist außerdem § 5 der Verordnung über Planung und Genehmigung von Maßnahmen auf dem Gebiet der elektronischen Datenverarbeitung vom 3. Dezember 1991, Amtsblatt 1992, Seite A 31, zu beachten.
4. Der Einsatz privater Datenträger auf privaten Geräten ist grundsätzlich untersagt. Schriftliche Ausnahmen kann nur die Dienststellenleitung erlassen.
5. Datenträger der Dienststelle müssen als solche von außen gut lesbar gekennzeichnet sein. Datenträger mit sensiblen Daten sollten auch über eine Datenträgernummer inventarisiert sein. Aus der Kennzeichnung sollte auch der Inhalt der Datenträger hervorgehen (farbige Aufkleber oder Filzstifte verwenden).

3.2. Technische Maßnahmen:

1. Um einen ungewollten Fremdzugriff zu erschweren, ist als Mindestanforderung die Aktivierung des Boot-Lock Paßwortes vorzusehen.
2. Um Programme und Daten auf transportablen Datenverarbeitungsgeräten und Datenträger zu schützen, sollte die jeweilige Dienststelle eine Software einsetzen, die über alle schutzwürdigen Programm-, Überlagerungs-, Treiber- und auch Datendateien (Ausnahme sind Dateien, die einer Veränderung unterliegen) immer konstant bleiben. Regelmäßige Kontrollen ermöglichen damit eine Überwachung aller Veränderungen auf dem jeweiligen Gerät und den verwendeten Datenträgern. Der Einsatz von Virenscannern ist sehr aufwendig, da eine regelmäßige Aktualisierung der Software nötig ist. Der erreichte Schutzeffekt ist nur sehr gering, weil nur

50 % der derzeit gängigen Viren erkannt werden. Des weitern entstehen täglich neue Viren. Hinweise zum Einsatz entsprechender Software gibt der Datenschutzbeauftragte der Landeskirche.

3. Unverlangt zugesandte Demonstrationssoftware jeglicher Art ist aus Sicherheitsgründen nicht zu installieren.
4. Es sind regelmäßig Datensicherungen anzufertigen. Dabei sollten die nachfolgenden Grundsätze beachtet werden:
   a) getrennte Sicherung von Programmen und Daten
   b) Durchführung der Datensicherung in mehreren Generationen (Großvater-Vater-Sohn-Prinzip)
   c) räumlich getrennte Aufbewahrung der Sicherheitskopien.
5. Der Dienststellenleiter hat die Mitarbeiter über ihre Rechte und Pflichten beim Umgang mit transportablen Datenverarbeitungsgeräten und Datenträgern regelmäßig zu unterrichten und die Mitarbeiter zu kontrollieren.

4. Personenbezogene Daten in transportablen Datenverarbeitungsgeräten

Eine dauernde Haltung von personenbezogenen Daten auf transportablen Geräten ist nicht zulässig. Bei einer vorübergehenden Verarbeitung aus technischen Gründen ist als Mindestanforderung die Aktivierung des Boot-Lock-Paßwortes vorzusehen. Ferner ist eine Datenschutzsoftware zu installieren, die nur dem autorisierten Benutzer eine Verwendung der Programme und Dateien gestattet. Diese Software muß das sogenannte Booten verhindern können. Entsprechende Software-Empfehlungen gibt der Datenschutzbeauftragte der Landeskirche. Transportable Datenverarbeitungsgeräte und Datenträger, auf denen personenbezogene Daten verarbeitet werden, sind in der Registermeldung der Dateien mit personenbezogenen Daten an den Datenschutzbeauftragten der Landeskirche zu melden.

5. Umgang mit Fremd-Datenträgern

Vor dem Einsatz von Fremddatenträgern muß überprüft werden, ob deren Einsatz unbedingt nötig ist. Sie sind grundsätzlich vor ihrem Einsatz zu überprüfen. Aus Sicherheitsgründen muß ein Einsatz derartiger Datenträger protokol-

liert werden. Dies gilt analog für die Weitergabe von Datenträgern der Dienststelle an andere Dienststellen (siehe Anlage). Vor einer Weitergabe dienststelleneigener Datenträger sollten diese mit dem Prüfsummenprogramm katalogisiert werden, um im Streitfall rechtlich geschützt zu sein.

6. Aufbewahrung transportabler Datenträger

Transportable Datenträger (insbesondere Disketten, Magnetbänder etc.) sind nach Dienstschluß stets verschlossen zu verwahren. Ausgenommen hiervon sind nur Wechselplatten und vergleichbare Medien.

Anlage

Datenträgernachweis
bei Verwendung von Fremddatenträgern bzw.
bei der Versendung eigener Datenträger

Datum:	E(ingang)/A(usgang)	Dateiträ-gernummer	Herkunft/ Empfänger	gepr. durch Unterschr.