Verordnung

über den Einsatz von Informationstechnologie (IT) in der Evangelisch-Lutherischen Landeskirche Sachsens (IT-VO)

Vom 9. August 2010 (ABl. 2010 S. A 169)

Aufgrund von § 32 Absatz 1 und 3 der Kirchenverfassung verordnet das Landeskirchenamt Folgendes:

Inhaltsübersicht *

§ 1
Anwendungsbereich

(1) Diese Rechtsverordnung regelt den Einsatz von Informationstechnologie (IT) in der Evangelisch-Lutherischen Landeskirche Sachsens. Dazu gehören im Wesentlichen folgende Bereiche:

- Einheitlichkeit von IT-Lösungen und IT-Beratung
- Einsatz von Programmen
- IT-Sicherheit
- Elektronische Information und Kommunikation
- Intranet der Landeskirche.

* nichtamtlich

(2) Nicht der kirchlichen Aufsicht unterstehenden, der Landeskirche jedoch zugeordneten rechtlich eigenständigen Einrichtungen wird empfohlen, diese Rechtsverordnung entsprechend anzuwenden.

§ 2
Grundsätze

(1) Die IT hat die sichere Verarbeitung und Übermittlung von Daten und Informationen zu gewährleisten. Sie dient der Erfüllung des kirchlichen Auftrags.

(2) Zur Verbesserung der Zusammenarbeit auf allen Ebenen der Landeskirche werden einheitliche IT-Lösungen angestrebt.

§ 3
Einheitlichkeit, Beratung

(1) In den Bereichen Meldewesen, Haushalts-, Kassen- und Rechnungswesen, Personalwesen, Gebäude-, Liegenschafts- und Friedhofswesen sowie E-Mail-Verfahren werden einheitliche IT-Lösungen eingesetzt. Das Landeskirchenamt legt nach Anhörung der betreffenden Stellen sowie des Datenschutzbeauftragten die einheitlichen IT-Lösungen fest.

(2) Vor wesentlichen Entscheidungen auf dem Gebiet der IT ist die Fachberatung des Landeskirchenamtes in Anspruch zu nehmen. Der Datenschutzbeauftragte ist frühzeitig zu informieren. Die IT-Fachberatung soll Unterstützung bei der Auswahl geeigneter Geräte- und Programmsysteme geben sowie die Nutzung von Rahmen- und/oder Lizenzverträgen ermöglichen. Darüber hinaus sollen damit die weitgehende Kompatibilität der eingesetzten Hilfsmittel gesichert, Hinweise zur Behandlung tangierender Problemstellungen (z. B. Prozessorganisation) gegeben und organisatorische Schwierigkeiten vermieden werden.

§ 4
Einsatz von Programmen

(1) Mindestvoraussetzungen für den Einsatz eines Anwendungsprogrammes sind, dass

- ein Anforderungsprofil und eine Programmdokumentation vorliegen
- keine datenschutzrechtlichen Bedenken bestehen sowie

- das Programm getestet worden ist und gültige Lizenzen vorhanden sind.

(2) Die Programme sollen mit bereits eingesetzten oder vorgesehenen kirchlichen Programmen kompatibel sein (Schnittstellen).

(3) Der Einsatz sowie die wesentlichen Änderungen von Programmen sind von dem Leitungsorgan der kirchlichen Körperschaft zu beschließen.

§ 5
IT-Sicherheit

(1) IT-Systeme und dienstliche Daten sind vor Verlust, unberechtigtem Zugriff und vor unerlaubter Änderung zu schützen (IT-Sicherheit), um ihre Verfügbarkeit, Integrität und Vertraulichkeit zu gewährleisten.

(2) Jede kirchliche Körperschaft ist verpflichtet, IT-Sicherheit zu gewährleisten. Dafür ist das jeweilige Leitungsorgan verantwortlich.

(3) Zur Umsetzung der IT-Sicherheit ist jede kirchliche Körperschaft verpflichtet, ein IT-Sicherheitskonzept zu erstellen und zu beschließen. Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen Gefährdungen von innen und außen enthalten. Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum jeweiligen Schutzbedarf, insbesondere im Hinblick auf Daten und IT-Systeme, stehen.

(4) Das dieser Verordnung anliegende Muster-IT-Sicherheitskonzept bildet die Beschlussgrundlage für die Kirchgemeinden und Kirchenbezirke und enthält insbesondere die Grundsätze der IT-Sicherheit. Davon abweichende IT-Sicherheitskonzepte sind dem Landeskirchenamt anzuzeigen.

§ 6
Elektronische Information und Kommunikation

(1) Das Internet darf dienstlich nur zur Erfüllung des kirchlichen Auftrags genutzt werden.

(2) Die Nutzung des landeskirchlichen Intranets dient zur Bereitstellung und zum Austausch dienstlicher Daten.

(3) Die Nutzung des landeskirchlichen E-Mailsystems dient zur dienstlichen Kommunikation. Alle kirchlichen Stellen und Mitarbeiter verwenden hierbei eine dienstliche E-Mail-Adresse mit der Domain „EVLKS.DE“ und kontrollieren regelmäßig den Posteingang.

§ 7
Intranet

(1) Alle kirchlichen Stellen und Mitarbeiter, die auf elektronischem Weg dienstliche Daten verarbeiten und abrufen, sind in das Intranet der Landeskirche einzubinden. Sie übermitteln die dienstlichen Daten über dieses Intranet.

(2) Die Freigabe für den Zugang zum Intranet erteilt das Landeskirchenamt. Voraussetzung für die Freigabe ist ein den Anforderungen des § 5 entsprechendes IT-Sicherheitskonzept.

(3) Der Zugang zum Intranet für den dienstlichen Gebrauch kann auch über private Rechner erfolgen. Beim Zugang zum Intranet über private Rechner ist insbesondere Folgendes sicherzustellen:

- geeignete Maßnahmen gegen Gefährdungen von innen und außen, insbesondere technische und organisatorische Maßnahmen zur Datensicherheit sowie
- Beachtung des kirchlichen Datenschutzrechtes.

(4) Sonstige von einer kirchlichen Körperschaft beauftragte Stellen, die im Interesse der kirchlichen Arbeit einen Zugang zum Intranet benötigen, können zugelassen werden.

(5) Personen und Stellen, die gemäß Absatz 3 und 4 Zugang zum Intranet haben, sind auf die Einhaltung des für die jeweilige kirchliche Körperschaft geltenden IT-Sicherheitskonzeptes zu verpflichten.

(6) Wird der im IT-Sicherheitskonzept definierte Standard oder der bereits dokumentierte Standard nicht eingehalten oder verändert, so dass die Sicherheit des Intranets beeinträchtigt wird, kann die Zugangsberechtigung vom Landeskirchenamt ausgesetzt oder widerrufen werden.

§ 8
Beteiligung

(1) Bei der Erstellung eines IT-Sicherheitskonzeptes gemäß § 5 Absatz 4 Satz 2 und bei der Entscheidung zur Auswahl von Programmen, über die personenbezogene Daten verwaltet werden, ist der Datenschutzbeauftragte gemäß Datenschutzgesetz der Evangelischen Kirche in Deutschland und den zu dessen Ausführung erlassenen Rechtsvorschriften in der jeweils geltenden Fassung zu beteiligen.

(2) Die Beteiligung der Mitarbeitervertretung gemäß Mitarbeitervertretungsgesetz in der jeweils geltenden Fassung ist zu gewährleisten.

§ 9
Datenverarbeitung im Auftrag

Die Vorschriften des Kirchengesetzes über den Datenschutz der EKD für die Datenverarbeitung im Auftrag finden entsprechend Anwendung. Vor einer Beauftragung ist die Genehmigung des Landeskirchenamtes einzuholen.

§ 10
Inkrafttreten, Außerkrafttreten

(1) Diese Rechtsverordnung tritt am 1. Oktober 2010 in Kraft.

(2) Gleichzeitig tritt die Verordnung über Planung und Genehmigung von Maßnahmen auf dem Gebiet der Elektronischen Datenverarbeitung vom 3. Dezember 1991 (ABl. 1992 S. A 31) außer Kraft.

Muster-IT-Sicherheitskonzept

für Körperschaften der Evangelisch-Lutherischen Landeskirche Sachsens

Inhaltsübersicht[*]

1 Präambel

Das Muster-IT-Sicherheitskonzept gemäß § 5 Absatz 4 Satz 1 IT-VO bildet die Beschlussgrundlage für alle Körperschaften der Evangelisch-Lutherischen Landeskirche Sachsens. Es enthält insbesondere die Grundsätze der IT-Sicherheit und bezweckt den Schutz von Daten, welche Eigentum dieser Körperschaften sind oder ihnen in der Erwartung anvertraut werden, dass sie diese Daten entsprechend schützen. Für diese Daten sollen Vertraulichkeit (Schutz vor Einsicht Unbefugter), Integrität (Unversehrtheit) und Verfügbarkeit sichergestellt werden.

Ein weiteres Ziel des IT-Sicherheitskonzeptes ist die Verfügbarkeit und Verlässlichkeit des Arbeitsmittels IT-System, welche die Voraussetzung für viele Bereiche des kirchlichen Handels darstellt.

2 Räumliche und zeitliche Geltung

Dieses IT-Sicherheitskonzept gilt für alle mobilen und stationären IT-Systeme der/des

[*] nichtamtlich

(Name und Sitz der Körperschaft)

sowie alle Computerprogramme und Daten, welche auf diesen IT-Systemen gespeichert sind oder verarbeitet werden. Auf die Einhaltung des IT-Sicherheitskonzeptes sind auch alle Dienstleister zu verpflichten, die Zugang zu diesen IT-Systemen haben.

Das IT-Sicherheitskonzept gilt ab … und ersetzt (soweit vorhanden) das IT-Sicherheitskonzept vom …

3 Grundsätze

3.1 Verantwortlichkeiten

Für jedes IT-System einschließlich der darauf gespeicherten Programme und Daten ist vom Leitungsorgan der Körperschaft eine natürliche Person als verantwortlich festzulegen. Die Verantwortung für ein IT-System kann übertragen werden, wenn dies schriftlich und nachvollziehbar dokumentiert wird. Ist kein Verantwortlicher festgelegt, liegt diese Verantwortung beim Leitungsorgan der Körperschaft.

Jeder Benutzer eines kirchlichen IT-Systems ist ungeachtet der vorstehenden Regelung für seine eigenen Handlungen verantwortlich und soll den Verantwortlichen für das IT-System durch umsichtiges Handeln unterstützen.

Die Gesamtverantwortung für die Einhaltung des IT-Sicherheitskonzeptes sowie der geltenden Datenschutzbestimmungen obliegt dem Leitungsorgan der Körperschaft.

3.2 Datenschutz

Daten sollen klassifiziert[1] werden, so dass ihr Schutzbedarf leicht und eindeutig erkennbar ist. Die Klassifizierung muss allen Personen mitgeteilt werden, welche Zugriff auf diese Daten erhalten.

Kirchliche und personenbezogene Daten sollen mit besonderer Sorgfalt behandelt werden. Das Klassifizieren und entsprechende Kenntlichmachen soll diese Daten als sensibel ausweisen.

Seelsorgerische Informationen dürfen in keinem Fall gespeichert werden.

Es gelten die Bestimmungen des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG.EKD).

[1] Die Regeln der Klassifizierung sind im CN abrufbar.

3.3 Computersicherheit

Alle IT-Systeme (z. B. Computer) müssen die folgenden Minimalanforderungen erfüllen:

1. Das IT-System ist mit einer Anti-Virus-Software ausgestattet, deren Datenbasis nicht älter als drei Tage ist. Die Anti-Virus-Software ist zu jeder Zeit aktiv.
2. Das IT-System installiert automatisch sicherheitsrelevante Aktualisierungen des Betriebssystems.
3. Nur Personen mit einem gültigen Benutzerkonto erhalten Zugriff auf das IT-System.
4. Das IT-System oder der Raum, in dem es sich befindet, sind vor unberechtigtem Zugang geschützt.

4 Fremdhardware

Die Verwendung von Fremdhardware (Computer und Peripherie) ist nicht gestattet.

Die Fälle nach § 7 Absatz 3 IT-VO sind davon nicht betroffen.

5 Benutzerkonten

Jeder Benutzer eines IT-Systems hat ein persönliches Benutzerkonto. Das Benutzerkonto ist durch ein Passwort gesichert, welches mindestens acht Zeichen lang ist und sowohl Groß- als auch Kleinbuchstaben enthält.

Das Passwort ist geheim zu halten, darf nicht hinterlegt, aufgeschrieben oder gespeichert werden. Inhaber eines Benutzerkontos dürfen dieses nicht weitergeben oder die mit dem Konto einhergehenden Berechtigungen missbrauchen.

6 Datensicherung

Von allen IT-Systemen soll in regelmäßigen Abständen eine Datensicherung angefertigt werden. Die Datenträger, welche die Datensicherung beinhalten, sollen sicher verwahrt werden.

7 Netzwerke

Alle IT-Systeme können in einem lokalen Netzwerk verbunden werden. Das Einbinden von Fremdhardware in lokale Netzwerke ist nicht gestattet und soll durch technische und/oder organisatorische Maßnahmen verhindert werden.

Lokale Netzwerke dürfen ausschließlich an das Corporate Network (CN) der Evangelisch-Lutherischen Landeskirche Sachsens angeschlossen werden, für das eigene Nutzungsbedingungen gelten. Verbindungen zu anderen Netzwerken, z. B. private Internetanschlüsse oder Funknetzwerke (WLAN), sind nicht gestattet.

Ort, Datum

Unterschriften, Dienstsiegel