Verordnung über den Einsatz von Informationstechnologie (IT) in der kirchlichen Verwaltung IT-Verordnung (ITVO)

Vom 16. Dezember 2004

(KABl. 2004 S. 306)

mit den Durchführungsbestimmungen zur Verordnung über den Einsatz von Informationstechnologie (IT) in der kirchlichen Verwaltung (DBIT-Verordnung – DBITVO) vom 1. Juli 2005 (KABl. 2005 S. 149)

Inhaltsübersicht[1]

1 Die Inhaltsübersicht ist nicht Bestandteil dieser Verordnung.

Die Kirchenleitung hat auf Grund des Artikels 159 Abs. 2 der Kirchenordnung der Evangelischen Kirche von Westfalen vom 1. Dezember 1953[1] (KABl. 1954 S. 25) in der Fassung vom 14. Januar 1999 (KABl. 1999 S. 1), zuletzt geändert durch das 43. Kirchengesetz zur Änderung der Kirchenordnung der Evangelischen Kirche von Westfalen vom 14. November 2002 (KABl. 2002 S. 336) in Verbindung mit § 27 Abs. 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993[2] (KABl. 1994 S. 34), zuletzt geändert durch das Erste Kirchengesetz zur Änderung des Kirchengesetzes über den Datenschutz in der Evangelischen Kirche in Deutschland vom 7. November 2002 (KABl. 2003 S. 157) sowie § 20 Abs. 1 des Kirchengesetzes über die Kirchenmitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder vom 10. November 1976[3] (KABl. 1977 S. 26) folgende Verordnung beschlossen:

§ 1
Anwendungsbereich

(1) Diese Verordnung regelt den Einsatz von Informationstechnologie (IT) in der Evangelischen Kirche von Westfalen (EKvW), insbesondere

- das Erstellen und Anwenden eines IT- Sicherheitskonzeptes,
- den Einsatz von Programmen,
- die Freigabe von Programmen,
- den Zugang und die Nutzung zum Intranet (Kirchliches Netz-Westfalen – KiNet-W).

(2) Der EKvW zugeordnete rechtlich eigenständige Einrichtungen können diese Verordnung ganz oder in Teilen für anwendbar erklären.

1. zu § 1 Abs. 1

Die ITVO gilt für alle Körperschaften des öffentlichen Rechts in der Evangelischen Kirche von Westfalen (EKvW), das heißt für Kirchengemeinden, Kirchenkreise, Landeskirche und Verbände.

2. zu § 1 Abs. 2

Rechtlich eigenständige Einrichtungen sind insbesondere diakonische oder sonstige Einrichtungen, die privatrechtlich in Form eines eingetragenen Vereins oder als Gesellschaft mit beschränkter Haftung oder als Stiftung organisiert sind.

---

1 Nr. **1**
2 Nr. **850**
3 Nr. **101**

§ 2
Grundsätze

(1) [1]Jede kirchliche Körperschaft ist verpflichtet ein IT-Sicherheitskonzept zu erstellen und anzuwenden. [2]Dabei sind die Mindestanforderungen des landeskirchlichen Muster-IT-Sicherheitskonzeptes unter Berücksichtigung der örtlichen Gegebenheiten zu übernehmen. [3]Es kann ein einheitliches IT-Sicherheitskonzept in einem Kirchenkreis verabschiedet werden. [4]Das IT-Sicherheitskonzept bedarf der Genehmigung des Landeskirchenamtes.

(2) Innerhalb der EKvW sind einheitliche IT-Lösungen zu entwickeln und einzusetzen.

(3) [1]Vor wesentlichen Entscheidungen auf dem Gebiet der IT ist die Beratung des Landeskirchenamtes in Anspruch zu nehmen. [2]Die oder der Betriebsbeauftragte oder die oder der örtlich Beauftragte für den Datenschutz ist frühzeitig zu informieren. [3]Entscheidungen auf dem Gebiet der IT sind dem Landeskirchenamt mitzuteilen.

(4) [1]Voraussetzung für den Einsatz von Anwendungsprogrammen ist, dass insbesondere

- ein Anforderungsprofil und
- eine Programmdokumentation vorliegen,
- keine datenschutzrechtlichen Bedenken bestehen,
- das Programm getestet worden ist und
- gültige Lizenzen vorhanden sind.

[2]Der Einsatz sowie die wesentlichen Änderungen von Programmen sind von dem Leitungsorgan der kirchlichen Körperschaft zu beschließen. [3]Die Entscheidungen können delegiert werden.

[4]Vorrangig sollen Programme eingesetzt werden, die bereits erfolgreich im Bereich der EKvW genutzt werden und für die möglichst ein Testat einer kirchlichen oder staatlichen Stelle vorliegt.

(5) Bei einem Einsatz von IT ist insbesondere für ausreichenden Virenschutz zu sorgen.

(6) Über die Erfordernisse des Datenschutzes hinaus sind alle dienstlichen Daten in geschützten Bereichen zu speichern.

(7) [1]Jede kirchliche Körperschaft hat eine IT-verantwortliche Person zu benennen. [2]Die Benennung für mehrere kirchliche Körperschaften ist zulässig.

3. zu § 2 Abs. 1

Vom Landeskirchenamt wird ein Muster-IT-Sicherheitskonzept zur Verfügung gestellt, das entsprechend den technischen Weiterentwicklungen fortgeschrieben und regelmäßig aktualisiert wird. Auf Grundlage des IT-Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) werden

- *IT- Bausteine beschrieben, die typischerweise in einer kirchlichen Körperschaft Anwendung finden,*
- *mögliche Gefährdungen und der Schutzbedarf der jeweiligen Bausteine dargestellt,*
- *die entsprechenden Maßnahmen für den sicheren Betrieb festgeschrieben.*

Das vom Landeskirchenamt erarbeitete Muster-IT-Sicherheitskonzept ist zu verwenden. Dabei können örtliche Besonderheiten ergänzend aufgenommen werden. Diese dürfen den Anforderungen des Muster-IT-Sicherheitskonzeptes nicht entgegenstehen. Das jeweilige Leitungsorgan muss das IT-Sicherheitskonzept beschließen.

Die erstmalige Erstellung des IT-Sicherheitskonzeptes für die kirchliche Körperschaft muss bis zum 31. Dezember 2006 erfolgen.

Dem Landeskirchenamt sind das IT-Sicherheitskonzept sowie der entsprechende Beschluss des Leitungsorgans zur Genehmigung vorzulegen. Im Einzelfall kann das Landeskirchenamt die Vorlage weiterer Unterlagen verlangen.

Ein einheitliches IT-Sicherheitskonzept in einem Kirchenkreis bedarf der Beschlüsse der betroffenen kirchlichen Körperschaften.

Der sich aus dem IT-Sicherheitskonzept ergebende Standard muss umgesetzt werden. Diese Umsetzung wird regelmäßig in Form von Gesprächen (Audits) überprüft. Das Audit auf Kirchenkreisebene führt grundsätzlich das Landeskirchenamt mit der IT-verantwortlichen Person des Kirchenkreises. Sofern Kirchengemeinden oder kirchliche Verbände im Kirchenkreis eigene IT-verantwortliche Personen benannt haben, führt die IT-verantwortliche Person des Kirchenkreises das Audit. Die in § 7 ITVO genannten Personen sind zu beteiligen. Das Ergebnis des Audits muss der kirchlichen Körperschaft schriftlich mitgeteilt werden. Festgestellte Mängel sind abzustellen.

4. zu § 2 Abs. 2

Die Anforderungen an die Einheitlichkeit betreffen den Einsatz von Programmen in vergleichbaren Einsatzbereichen und die IT – Struktur für den dienstlichen Datenaustausch.

5. zu § 2 Abs. 3

Wesentliche Entscheidungen auf dem Gebiet der IT sind vor allem:

- *Aufbau neuer IT-Infrastrukturen,*
- *Wechsel zu anderen Betriebssystemen,*
- *Einsatz neuer Anwendungsprogramme,*
- *Einsatz freigabepflichtiger Programme,*
- *Nutzung neuer Kommunikationstechnik.*

Im Rahmen der Beratung prüft das Landeskirchenamt, ob bereits entsprechende IT-Lösungen in der EKvW im Einsatz sind oder die geplante IT-Lösung über eine landeskirchliche Anwendergruppe geprüft und bewertet werden kann.

6. zu § 2 Abs. 4

Anwendungsprogramme im Sinne der ITVO sind Standardsoftware (Standardbürosoftware wie z.B. Textverarbeitung, Tabellenkalkulation; funktionsorientierte Standardsoftware wie z.B. Finanzbuchhaltung, Friedhofsverwaltung) und Individualsoftware.

Das Anforderungsprofil beschreibt Funktionen, Daten und Schnittstellen, die zur Aufgabenerfüllung in dem jeweiligen Arbeitsbereich vorhanden sein müssen. Die Kompatibilität zu Betriebssystemen und Anwendungsprogrammen ist sicherzustellen.

Die Programmdokumentation (Handbücher und/oder Online-Dokumentationen) muss die Aspekte des Anforderungsprofils beinhalten. Bei Individualsoftware soll über die Programmdokumentation hinaus eine Regelung über die Hinterlegung des Quellcodes getroffen werden.

Bei Anwendungsprogrammen, mit denen personenbezogene Daten verarbeitet oder übermittelt werden, bestehen keine datenschutzrechtlichen Bedenken, wenn

- *die rechtliche Zulässigkeit der Erhebung, Speicherung und Übermittlungen der personenbezogenen Daten unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit festgestellt wird,*
- *den Auskunftsrechten (z.B. nach § 15 DSG-EKD) entsprochen werden kann,*
- *die Berichtigung, Löschung und Sperrung personenbezogener Daten (z.B. nach § 16 DSG-EKD) möglich ist,*
- *ausreichende technische und organisatorische Datenschutzmaßnahmen unter Berücksichtigung des Schutzbedarfs und der Anforderungen der Anlage zu § 9 Abs. 1 DSG-EKD vorliegen.*

Das Anwendungsprogramm muss vor dem Hintergrund des Anforderungsprofils getestet werden.

7. zu § 2 Abs. 5

Ausreichender Virenschutz bedeutet regelmäßiger und insbesondere aktueller Schutz vor Viren und anderen schädigenden Programmen (z.B. Würmern, Trojanern). Dieser Virenschutz kann als Dienstleistung durch das Kreiskirchenamt oder durch externe Stellen oder in eigener Verantwortung erfolgen.

Sicherheitslücken in Betriebssystemen, in einzelnen Programmen oder Programmteilen sind unverzüglich zu schließen.

8. zu § 2 Abs. 6

Zur Speicherung dienstlicher Daten müssen ausreichende organisatorische und technische Maßnahmen entsprechend dem IT- Sicherheitskonzept einen möglichen unberechtigten Zugriff ausschließen.

Sofern dienstliche Rechner nicht in einem lokalen Netzwerk (LAN) betrieben werden, dürfen dienstliche Daten nur in verschlüsselten Verzeichnissen auf der Festplatte oder auf externen Medien (z.B. Diskette, optisches Laufwerk, USB-Speichermedium) gespeichert werden. Sofern externe Speichermedien genutzt werden, müssen sie nach Speicherung verschlossen aufbewahrt werden.

Es ist sicherzustellen, dass nur berechtigte Personen Zugang zu den Daten haben.

9. zu § 2 Abs. 7

IT-verantwortliche Personen sollen Mitarbeitende der Körperschaft sein, die für die Arbeitsfelder IT und IT-Sicherheit zuständig sind.

§ 3
Freigabe von Programmen

(1) [1]Programme für die Bereiche Meldewesen, Kirchenbuchwesen, Personalwesen sowie Haushalts-, Kassen- und Rechnungswesen müssen vor Einsatz in den einzelnen kirchlichen Körperschaften freigegeben sein. [2]Für weitere Bereiche kann das Landeskirchenamt die Freigabepflicht beschließen.

(2) [1]Anträge auf Freigabe können nur durch kirchliche Körperschaften gestellt werden. [2]Über den Antrag auf Freigabe entscheidet das Landeskirchenamt. [3]Die Freigabe erfolgt grundsätzlich für die gesamte Landeskirche, im Ausnahmefall für eine einzelne kirchliche Körperschaft. [4]Die Freigabe kann mit Auflagen und Nebenbestimmungen verbunden werden.

(3) [1]Programme können freigegeben werden, soweit sie fachlichen, technischen sowie datenschutzrechtlichen Anforderungen entsprechen und sie nicht dem Grundsatz der Einheitlichkeit widersprechen. [2]Das Landeskirchenamt kann im Benehmen mit der antragsstellenden Körperschaft dazu ein Gutachten in Auftrag geben. [3]Alle dabei entstehenden Kosten sind durch die antragstellende Körperschaft zu tragen.

(4) Das Landeskirchenamt kann von einer Prüfung des jeweiligen freigabepflichtigen Programms ganz oder teilweise absehen, wenn durch die antragstellende Körperschaft qualifizierte Freigabetestate anderer kirchlicher Körperschaften oder anderer Prüfstellen vorgelegt werden.

(5) Wesentliche Änderungen freigegebener Programme sind dem Landeskirchenamt mitzuteilen.

(6) Wenn die Voraussetzungen für die Freigabe eines Programms nicht mehr gegeben sind, kann das Landeskirchenamt die Freigabe widerrufen.

10. zu § 3

Gemäß Ziffer 5 dieser Durchführungsbestimmung ist rechtzeitig vor der Freigabe die Beratung des Landeskirchenamtes einzuholen. Im Rahmen dieser Beratung werden der an-

tragstellenden Körperschaft die Kriterien für eine etwaige Freigabe gemäß § 3 Abs. 3 ITVO benannt. Diese Kriterien müssen bei den Anbietergesprächen und Programm-Präsentationen berücksichtigt werden.

11. zu § 3 Abs. 5

Wesentlichen Änderungen sind insbesondere fachliche (Erweiterung des Programms um zusätzliche Module, Änderung des Funktionsumfangs) und technische Änderungen (Änderung der Datenstruktur oder Datenbank) und Änderungen, die den Datenschutz berühren.

§ 4
Intranet KiNet-W

(1) Alle kirchlichen Stellen, die auf elektronischem Weg dienstliche Daten verarbeiten oder abrufen, sind in KiNet-W einzubinden.

(2) Die elektronische Übermittlung von dienstlichen Daten erfolgt innerhalb der EKvW über KiNet-W.

12. zu § 4 Abs. 1

Auch private Rechner im Sinne von § 5 Abs. 3 ITVO sind als kirchliche Stellen anzusehen.

13. zu § 4 Abs. 2

Wenn dienstliche Daten an außerkirchliche Stellen, die nicht in KiNet-W eingebunden sind, weitergeleitet werden müssen, ist eine größtmögliche Datensicherheit zu gewährleisten. Einzelheiten sind im IT-Sicherheitskonzept zu regeln.

§ 5
Zugang zum Intranet KiNet-W

(1) $_1$Die Freigabe für den Zugang zu KiNet-W erteilt das Landeskirchenamt. $_2$Voraussetzung für die Freigabe ist ein genehmigtes IT-Sicherheitskonzept.

(2) Wird der im genehmigten IT-Sicherheitskonzept definierte Standard oder der bereits dokumentierte Standard nicht eingehalten oder verändert, sodass die Sicherheit von KiNet-W gefährdet wird, kann die Zugangsberechtigung vom Landeskirchenamt widerrufen werden.

(3) $_1$Der Zugang zu KiNet-W für den dienstlichen Gebrauch kann auch über private Rechner erfolgen. $_2$Die Vorgaben des für die jeweilige kirchliche Körperschaft geltenden IT- Sicherheitskonzeptes sind einzuhalten. $_3$Beim Zugang zu KiNet-W über private Rechner ist durch Vereinbarung insbesondere Folgendes zu regeln:

- ausreichender Virenschutz,
- Anwendung des kirchlichen Datenschutzrechtes,

- technische und organisatorische Maßnahmen zur Datensicherheit und zum Datenschutz.

(4) [1]Sonstige von einer kirchlichen Körperschaft beauftragte Stellen, die im Interesse der kirchlichen Arbeit einen Zugang zu KiNet-W benötigen, können zugelassen werden. [2]Die Vorgaben des für die jeweilige kirchliche Körperschaft geltenden IT- Sicherheitskonzeptes sind einzuhalten.

14. zu § 5 Abs. 1

Für die in § 1 Abs. 2 ITVO genannten kirchlichen Stellen kann die Freigabe erteilt werden, wenn die für den Zugang erforderlichen Vorgaben des Muster-IT-Sicherheitskonzeptes eingehalten werden.

15. zu § 5 Abs. 3

Insbesondere für Pfarrerinnen und Pfarrer, Presbyterinnen und Presbyter sowie für Mitarbeitende der kirchlichen Verwaltungen kann der Zugang auch über einen privaten Rechner erfolgen, wenn eine IT- Verpflichtungserklärung abgegeben wird. Dadurch muss insbesondere der oder dem Datenschutzbeauftragten der EKvW, der oder dem örtlich Beauftragten für den Datenschutz sowie der IT-verantwortlichen Person ein Zugriff auf den Rechner ermöglicht werden. Vom Landeskirchenamt wird eine Muster-IT-Verpflichtungserklärung zur Verfügung gestellt.

16. zu § 5 Abs. 4

Sonstige von einer kirchlichen Körperschaft beauftragte Stellen sind insbesondere externe Dienstleister, die beispielsweise IT- Service für kirchliche Körperschaften durchführen. § 11 DSG-EKD findet entsprechend Anwendung.

§ 6
Aufgaben der IT- verantwortlichen Person

(1) Die IT-verantwortliche Person der jeweiligen Körperschaft hat das IT-Sicherheitskonzept zu erstellen, anzupassen sowie Erweiterungen aufzunehmen.

(2) Die Anwendung des IT-Sicherheitskonzeptes ist von der IT-verantwortlichen Person zu kontrollieren und zu überwachen.

(3) [1]Personen, die gemäß § 5 Abs. 3über einen privaten Rechner Zugang zu KiNet-W haben, und sonstige Stellen gemäß § 5 Abs. 4 sind für die Einhaltung des für die jeweilige kirchliche Körperschaft geltenden IT-Sicherheitskonzeptes verantwortlich. [2]Sie erhalten dazu Beratung und Unterstützung von der IT-verantwortlichen Person.

17. zu § 6 Abs. 1

Die Aufgaben ergeben sich aus einer Dienstanweisung. Die vom Landeskirchenamt erarbeitete Muster-IT-Dienstanweisung ist zu Grunde zu legen.

§ 7
Beteiligung der oder des Betriebsbeauftragten oder der oder des örtlich Beauftragten für den Datenschutz

Bei der Erstellung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl von Programmen, über die personenbezogene Daten verwaltet werden, ist die oder der Betriebsbeauftragte oder die oder der örtlich Beauftragte für den Datenschutz frühzeitig zu beteiligen.

§ 8
Datenverarbeitung im Auftrag

[1]Die Vorschriften des Kirchengesetzes über den Datenschutz der EKD für die Datenverarbeitung im Auftrag finden entsprechend Anwendung. [2]Vor einer Beauftragung ist die Genehmigung des Landeskirchenamtes einzuholen.

§ 9
Schlussbestimmungen

(1) Das Landeskirchenamt kann Durchführungsbestimmungen zu dieser Verordnung erlassen.

(2) Diese Verordnung tritt am 1. Januar 2005 in Kraft.

(3) Gleichzeitig tritt die Verordnung über den Einsatz von elektronischer Datenverarbeitung in der kirchlichen Verwaltung in der Fassung der Bekanntmachung vom 13. Oktober 1994 außer Kraft.