

Begründung
zum Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der EKKW
Vom 24. November 2014

A. Allgemeines:

Elektronische Datenverarbeitung spielt in der Evangelischen Kirche von Kurhessen-Waldeck seit den 1980er Jahren eine immer bedeutendere Rolle. Dabei hat die Datenverarbeitung keinen Selbstzweck. Vielmehr ändern sich die Anforderungen an heutige Arbeitsplätze, interne Vorgänge und Abläufe, die Koordinierung mit externen Verfahren und Behörden. Kommunikations- und Abstimmungsbedürfnisse innerhalb einer flächenverteilten Organisation nehmen zu. Damit gehen massiv gestiegene Bedürfnisse und Anforderungen des Datenschutzes einher.

Bereits vor der Einführung des Intranets, insbesondere aber mit dessen Einführung ab den Jahren 2007/2008, ergaben sich verschiedenste Veränderungen in der Arbeitsweise der Evangelischen Kirche von Kurhessen-Waldeck im Bereich Datenverarbeitung und elektronischer Kommunikation. Vor allem die landeskirchenweite digitale Vernetzung mit der Zusammenführung aller Standorte in einem abgesicherten Netz (Intranet) erfordert diverse Vorkehrungen und Regelungen. Im optimalen Falle werden bereits im Vorfeld von Veränderungen rechtliche Regelungen gefunden. So wurden im Zuge der Einführung des Intranets diverse rechtliche Bedingungen angepasst oder neugeschaffen, die den Dienstbetrieb sichern, den Datenschutz aufrechterhalten und die Verfügbarkeit aller technischen Komponenten garantieren helfen.

Zugleich wurde deutlich, dass die bisherigen Regelungen des EDV-Gesetzes von 1989 und der weiteren IT-bezogenen Verordnungen nicht mehr den aktuellen Anforderungen entsprechen. Im neu zu fassenden IuK-Gesetz werden alle nach heutigem Stand der Technik erforderlichen rechtlichen Voraussetzungen, die einer gesetzlichen Regelung bedürfen, im Sinne einer aktuellen und zukunftsweisenden Lösung zusammengefasst. Insbesondere im Hinblick auf die Anforderungen an IT-Sicherheit werden neue Standards umgesetzt, die bereits vom EKD-Gesetzgeber im neuen Datenschutzrecht der EKD definiert sind.

Hierbei spielt die Frage der Corporate Identity und damit einer einheitlichen E-Mail eine technisch kleine, in der Außenwahrnehmung und vor allem dem Datenschutz jedoch zentrale Rolle. Ferner sind Fragen des sicheren und datenschutzkonformen Intranetzzugriffs von Anwendern zu beantworten. Schließlich sind Aspekte der zunehmenden Nutzung privater Geräte zu dienstlichen Zwecken zu bewerten und zu regeln. Technisch stehen vielfältige Möglichkeiten zur Verfügung. Hier bedarf es einer handhabbaren und praxisorientierten Ausgestaltung.

Um die Bedeutung dieser Fragen im Hinblick auf Datenschutz, Datensicherheit und IT-Sicherheit zu würdigen, werden alle wesentlichen Fragen, die bislang auf verschiedenen Normebenen (Kirchengesetz mit geringem Regelungsinhalt, Rechtsverordnung des Rates, Richtlinien des Landeskirchenamts) geregelt waren, in einem IuK-Gesetz zusammengefasst. Das Landeskirchenamt kann für weitere Detailregelungen Ausführungsvorschriften erlassen (§ 7). Unberührt bleibt die Regelungskompetenz des Rates zum Erlass von Durchführungsverordnungen zum Datenschutzgesetz der EKD aufgrund von § 1 Abs. 2 der Verordnung über die Zustimmung der Evangelischen Kirche von Kurhessen-Waldeck zum

Kirchengesetz der Evangelischen Kirche in Deutschland über den Datenschutz vom 10. November 1977 vom 6. Januar 1978 (KABl. S. 12).

B. Zu den Vorschriften im Einzelnen:

zu § 1:

§ 1 regelt im Sinne der üblichen Gesetzssystematik den Anwendungsbereich sowie den Geltungsbereich des Gesetzes. Das vorliegende IuK-Gesetz gilt in der gesamten Landeskirche mit ihren öffentlich-rechtlichen Körperschaften einschließlich deren unselbständiger Werke und Einrichtungen. Gemäß Absatz 2 können zugeordnete selbständige Werke und Einrichtungen die Anwendung des Gesetzes beschließen.

Da die Regelungen des Gesetzes die bestehenden Vorschriften zum Datenschutz sowie zum Mitarbeitervertretungsrecht ergänzen sollen, bleiben diese Regelungen ausdrücklich unberührt.

zu § 2:

§ 2 enthält zentrale Grundsätze zum Einsatz von Informations- und Kommunikationstechnik im kirchlichen Dienst. Diese Grundsätze werden in den folgenden Gesetzesvorschriften konkretisiert.

Jeder Einsatz von IuK-Technik hat Unterstützungsfunktion für den kirchlichen Auftrag. Dabei steht der Grundsatz der Sicherheit der automatisierten Datenübermittlung und -verarbeitung im Vordergrund. Diesem Grundsatz sowie weiteren genannten Zielen dient unter anderem der Einsatz landeskirchlich einheitlicher IuK in wichtigen Bereichen, insbesondere dort, wo personenbezogene Daten verarbeitet werden (vgl. § 3). Aus Sicherheitsaspekten ist eine Vereinheitlichung von IT-Hardware in der Landeskirche nicht im Fokus. Allerdings können aus Gründen der Sicherheit, der Wartbarkeit sowie aufgrund bestimmter Systemvoraussetzungen für einheitliche Dienste bestimmte Standards an die dienstlich genutzte Hardware gestellt werden.

zu § 3:

Das IuK-Gesetz verwendet die Begriffe Informations - und Kommunikationssystem, -dienst und -programm. Diese sind im Sinne des Gesetzes wie folgt definiert:

System ist als Gesamtheit aller eingesetzten Computersysteme zu verstehen. Das Computersystem der EKKW bildet ein zentral basiertes Intranet, das der Informationsverarbeitung (die Ein- und Ausgabe der Daten) dient. Hierunter sind nicht mehr nur rein stationäre Systeme zu fassen, sondern sämtliche dienstlich genutzte Computer, mobile Geräte und Netzwerkkomponenten als Gesamtkonstrukt. Besondere Bedeutung kommt dabei den Hintergrundsystemen (Server und Netzwerk) zu, die dem Nutzer einen Dienst (s. unten) als eine in sich geschlossene Funktionskomponente zur Verfügung stellen und dabei maßgebliche Aufgaben des Datenschutzes vorhalten, ohne dass sich der Nutzer selber darum kümmern muss.

Der Begriff Dienst beschreibt eine technische, autarke Einheit, die zusammenhängende Funktionalitäten zu einem Themenkomplex bündelt und über eine klar definierte Schnittstelle zur Verfügung stellt. Typische Beispiele sind hier Webdienste, die Funktionalitäten für Dritte beispielsweise über Intranet verfügbar machen (z. B. Bündelung von Funktionen und Inhalten im Intranetportal, E-Mail-Nutzung über Gerätegrenzen hinweg, Virens Scanneraktualisierung). Im Sinne des § 3 IuK-G wird hierunter auch die Gruppe der Dienstprogramme gefasst, die für den Nutzer beziehungsweise Systemverwalter eines Computers allgemeine, oft systemnahe Aufgaben ausführt (Umsetzung der Vorgabe „Viren scannen“ oder „Systemupdates holen“). Jeder dienstliche Computer in der EKKW nutzt eine Reihe von Dienstprogrammen, die meistens auf eine ganz bestimmte Aufgabe spezialisiert

sind. Dienstprogramme sind im Gegensatz zu Anwendungsprogrammen (s. unten § 4) Teil der Systemsoftware.

Mit Anwendungsprogrammen oder auch Anwendungssoftware, kurz: Programme (in der mobilen Welt Application bzw. App), werden Computerprogramme bezeichnet, die genutzt werden, um eine nützliche oder gewünschte nicht systemtechnische Funktionalität zu bearbeiten oder zu unterstützen. Sie dienen der Lösung von Benutzerproblemen. Beispiele für Anwendungsgebiete sind: Textverarbeitung, Bildbearbeitung, Tabellenkalkulation oder Finanzbuchhaltung. Eine besondere Form von Anwendungssoftware sind Webanwendungen. Auf diese wird vom Arbeitsplatzrechner oder Mobilgerät über einen Webbrowser zugegriffen und sie laufen im Browser ab.

Das Gesetz definiert mit dem Finanz-, Melde-, Personal-, Gebäude- und Liegenschaftswesen, die Bereiche, in denen bereits heute eine einheitliche luK-Lösung landeskirchenweit zum Einsatz kommt. Die dienstliche Kommunikation durch E-Mail und sonstige Datenverarbeitung über das Intranet einschließlich der technischen Hintergrundsysteme, sowie die IT-Sicherheit (z.B. Firewall, Antivirenlösungen) sind ebenso bereits einheitlich festgelegt.

In weiteren Themenfeldern kann in Zukunft eine einheitliche Lösung angezeigt sein. Nach einer zeitlich vorlaufenden repräsentativen Beteiligung der Nutzergruppen neuer Dienste insbesondere auch der Kirchenkreise und -gemeinden obliegt die Entscheidung für ein einheitliches neues System dem Landeskirchenamt.

zu Absatz 4 bis 6:

In allen Bereichen, in denen bislang keine einheitlichen luK-Systeme, -dienste oder Programme eingesetzt werden, beschließen die Leitungsorgane der kirchlichen Körperschaften über den Einsatz und Veränderungen von luK-Lösungen. Zuvor ist die Beratung des Landeskirchenamtes obligatorisch. Bei neuen, nicht freigegebenen Lösungen ist eine Freigabe durch das Landeskirchenamt erforderlich.

Die standardmäßig eingesetzte Software, z.B. im Bereich der Office-Produkte, wird für alle Anwender von der Landeskirche freigegeben. Für wesentliche Änderungen freigegebener Programme gelten die Vorgaben entsprechend.

zu § 4:

§ 4 nimmt den (datenschutzrechtlichen) Grundsatz der IT-Sicherheit aus § 9 des Datenschutzgesetzes der EKD (DSG-EKD i. d. F. der Bekanntmachung vom 1. Januar 2013, ABl. EKD S. 2) zur Verdeutlichung auf, der jede kirchliche Stelle zur Gewährleistung von IT-Sicherheit verpflichtet. Zur Ausführung des § 9 DSG.EKD wird der Rat der EKD in nächster Zeit mit Zustimmung der Kirchenkonferenz eine Rechtsverordnung mit weiteren Vorgaben erlassen, die die Evangelische Kirche von Kurhessen-Waldeck ebenfalls bindet.

Jede kirchliche Stelle, d.h. im Rahmen dieses Gesetzes neben der Landeskirche jede kirchliche Körperschaft, muss künftig ein IT-Sicherheitskonzept beschließen und eine IT-Sicherheitsbeauftragung aussprechen. Die Landeskirche wird im Rahmen einer einheitlichen Sicherheitsstruktur auf der Grundlage von EKD-weit vorgesehenen Mustern eigene Muster für IT-Sicherheitskonzepte vorgeben. IT-Sicherheitsbeauftragte können für mehrere kirchliche Stellen gemeinsam bestellt werden. Sie unterstützen das für die IT-Sicherheit verantwortliche Leitungsorgan durch Kontrolle, Beratung und Empfehlungen, Untersuchung von Sicherheitsvorfällen und Schulung.

Als ein wesentlicher Bestandteil von IT-Sicherheit untersagt das Gesetz die private Nutzung dienstlicher Geräte. Von diesem Grundsatz kann nur zugunsten einer - regelmäßig zeitlich beschränkten - Nutzung abgewichen werden, die vom Dienstvorgesetzten, z.B. im Rahmen einer Dienstvereinbarung, zugelassen werden kann.

zu § 5:

§ 5 nimmt im Wesentlichen die Vorschriften der bisherigen Intranet-/Internet-VO vom 12. November 2010 (KABl. 2011, S. 27) auf. Die Vorschrift beinhaltet grundsätzliche Regelungen zur Nutzung des landeskirchlichen Intranets. „Intranet“ ist hier umfassend als die technische Plattform zu verstehen, über die sowohl von dienstlichen als auch von privaten Endgeräten alle dienstlichen IuK-Dienste und die elektronische Kommunikation abgewickelt werden. Die auf Grund dieser Verordnung erlassenen Richtlinien (Intranetrichtlinie vom 8. Februar 2011, KABl. S. 80, Zertifizierungsrichtlinie PKI vom 21. Dezember 2010, KABl. 2011, S. 28) behalten ihre Gültigkeit. Neu aufgenommen ist als gesetzliche Verpflichtung die Nutzung der einheitlichen E-Mail-Adresse „@ekkw.de“.

zu § 6:

Bereits seit langem werden private Endgeräte auch zu dienstlichen Zwecken genutzt. Die Vorschrift schafft die grundsätzliche gesetzliche Möglichkeit der Zulassung der Nutzung privater Geräte durch Mitarbeitende. Zu unterscheiden ist hierbei zum einen die Nutzung dienstlicher Daten, die sich auf zentralen Servern befinden und auf die mittels einer sicheren Einwahlplattform auf das landeskirchliche Intranet zugegriffen wird. Diese Zugänge sind derzeit vor allem CAG (Citrix Access Gateway), OWA (Outlook Web App) und intranetmobil.ekkw.de. Dieser Zugriff kann grundsätzlich über das Internet von jedem Endgerät aus erfolgen und kann zentral auf Antrag zugelassen werden. (Hiervon zu unterscheiden ist der Telekommunikationsdienst, z.B. WLAN, über den eine Internetverbindung zum Datentransfer hergestellt wird.)

Zum anderen können dienstliche Daten unmittelbar auf privaten Geräten gespeichert und verarbeitet werden, z.B. mittels eines Übertragungsmediums wie externer Festplatte oder USB-Stick. Dies ist im Sinne der Datensicherheit ausgeschlossen, da ein unberechtigter Zugriff nicht kontrollierbar ist. Allerdings besteht in Zeiten zunehmender mobiler Datennutzung Bedarf nach einer synchronisierten Erreichbarkeit bestimmter dienstlicher Daten, insbesondere E-Mails, Kontakte, Kalender und Aufgaben. Die lokale Speicherung dieser Daten, die regelmäßig Personenbezug aufweisen, auf privaten mobilen Endgeräten bedarf einer besonderen rechtlichen Legitimierung und gesteigerter Sicherheitsmechanismen.

Absatz 3 legt bestimmte grundsätzliche Voraussetzungen hierfür fest. Um den kirchlichen Datenschutz im Hinblick auf personenbezogene Daten auch auf privaten Endgeräten zu gewährleisten, ist eine verlässliche zentrale softwaregesteuerte Verwaltung der Geräte durch ein sogenanntes „Mobile Device Management“ erforderlich, die auf allen zugelassenen Geräten die definierten Sicherheitsstandards unabhängig vom Betriebssystem gleichartig umsetzt. Dieses bedingt insbesondere einen Zugangsschutz mit Benutzererkennung und Passwort sowie den Ausschluss sicherheitsgefährdender schädlicher Applikationen. Die rechtliche Absicherung dieses technischen Rahmens erfolgt durch eine Vereinbarung der Landeskirche mit dem Nutzer oder der Nutzerin. Dies ist angezeigt, um die gegenseitigen Rechte und Pflichten insbesondere im Hinblick auf Haftung, Datenschutz und Kosten bei der dienstlichen Einbindung eines privaten Gerätes verbindlich zu regeln.

Auf privaten Endgeräten bleibt wie bisher (§ 4 Abs. 1 EDV-VO) die Speicherung von Seelsorgedaten sowie Daten aus diakonischer Arbeit generell unzulässig. Damit soll die Speicherung sensibler personenbezogener Daten mit dienstlichem Hintergrund auf privaten Endgeräten vermieden werden.

Andere Daten, wie z.B. aus dem Gebäudebestand oder Finanzdaten, können hingegen grundsätzlich im definierten Rahmen auch auf privaten Geräten verarbeitet werden. Allerdings ist auch der technische Zugriff hierauf über dienstliche Programme ausschließlich über die Einwahlplattform der Landeskirche gestattet.

Mitbestimmungsrechtliche Anforderungen, insbesondere § 40j MVG.EKD, sind zu beachten, jedoch nicht Regelungsgegenstand dieses Gesetzes.

zu § 7:

Weitere Einzelregelungen und zur Durchführung des Gesetzes, insbesondere zur Internet- und Intranetnutzung, kann das Landeskirchenamt im Wege von Verwaltungsvorschriften erlassen. Die bereits existierende Intranetrichtlinie vom 8. Februar 2011 (KABl. S. 80) und die Zertifizierungsrichtlinie vom 21. Dezember 2010 (KABl. 2011 S. 28) bleiben in Kraft (zur Weitergeltung untergesetzlicher Regelungen bei Fortfall der Ermächtigungsgrundlage vgl. nur BVerfG, Beschl. v. 3.12.1958 - 1 BvR 488/57) und werden bei Bedarf angepasst.

zu § 8:

Mit dem Inkrafttreten zum 1. Januar 2015 wird die erforderliche Anpassung bzw. der Erlass untergesetzlicher Regelungen ermöglicht. Das EDV-Gesetz sowie die genannten Rechtsverordnungen werden inhaltlich durch das hiesige Gesetz abgelöst und können außer Kraft treten.