Landessynode
Ev. Landeskirche Anhalts
7. Tagung - 23. Legislaturperiode
17. und 18. April 2015 in Köthen

EVANGELISCHE
Landeskirche
Anhalts

Die Landessynode hat beschlossen:

Erstes Kirchengesetz zur Änderung der IT-Sicherheitsordnung vom ... April 2015

§ 1

Die Ordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik (IT) (IT-Sicherheitsordnung) vom 8. Juli 2013 wird wie folgt geändert:

1. Die Präambel erhält folgenden Wortlaut:

Präambel

Der Gebrauch von Computern und Netzen ist für die haupt-, neben- und ehrenamtlichen Mitarbeitenden in der Evangelischen Landeskirche Anhalts zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtert der Computer viele Tätigkeiten und manche Arbeiten wären ohne den Einsatz von Computern gar nicht mehr denkbar. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer verletzen. Daher haben alle Nutzer sorgfältig und verantwortungsvoll unter Einhaltung der rechtlichen Vorschriften Computer und Netze zu nutzen.

In dieser Vorschrift wird aufgezeigt, welche Mindeststandards für den Betrieb eines Computers bzw. eines Netzes verbindlich sind und welche Konsequenzen bei Nichteinhaltung der IT-Sicherheitsordnung gezogen werden. Zweck der IT-Sicherheitsordnung ist es, diese Themenkreise zu formalisieren und allen Benutzern eine einheitliche Grundlage zu bieten, anhand derer entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind.

Die Informationssicherheit ist systematisch und umfassend an die technischen und rechtlichen Entwicklungen anzupassen, damit eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten erreicht wird. Dabei sind die umgesetzten Lösungen praxistauglich und ausreichend komfortabel zu gestalten, damit sie von den Mitarbeitenden auch in der täglichen Arbeit nicht als belastend, sondern als sinnvoll akzeptiert werden.

Auf Grund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die IT-Sicherheitsordnung soll für IT-Sicherheit sensibilisiert werden. Die IT-Sicherheitsordnung soll als Richtschnur für das eigene Handeln, sowie für das Beurteilen des Handelns der Anderen dienen.

2. § 2 erhält folgenden Wortlaut:

§ 2
IT-Sicherheitsstandard

(1) Die mit der Informationstechnik (IT) erhobenen und verarbeiteten Daten sind insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes zu schützen (IT-Sicherheit), um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

(2) Jede kirchliche Stelle im Sinne des § 1 Absatz 2 Satz 1 des Datenschutzgesetzes der EKD (DSG-EKD) hat das vom Landeskirchenrat erstellte aktuelle IT-Sicherheitskonzept der Landeskirche umzusetzen. Der Landeskirchenrat hat das IT-Sicherheitskonzept regelmäßig zu aktualisieren.

(3) Bei der Erstellung und der regelmäßigen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, ist soweit vorhanden, der Betriebsbeauftragte für den Datenschutz frühzeitig zu beteiligen. Anderenfalls ist der landeskirchliche Beauftragte nach § 18 DSG-EKD zu beteiligen.

(4) Der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard orientiert sich an den jeweiligen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz oder einem vergleichbaren Standard. Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen Gefährdungen von innen und außen enthalten. Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Schutzbedarf der Daten und der IT-Systeme stehen.

(5) Die Evangelische Landeskirche Anhalts führt für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit, für die das DSG-EKD gilt (gemäß § 1 Absatz 2 Sätze 3 und 4 DSG-EKD). Der Landeskirchenrat stellt Muster-IT-Sicherheitskonzepte insbesondere für die Landeskirche, die Kirchengemeinden und die im Satz 1 erwähnten Werke und Einrichtungen zur Verfügung, die die Mindestanforderungen der IT-Sicherheit unter Berücksichtigung der örtlichen und sachlichen Gegebenheiten darstellen und einzuhalten sind.

3. § 3 Absatz 2 erhält folgenden Wortlaut:

(2) Die mit der Informationstechnik erhobenen, verarbeiteten und genutzten Daten sind zu schützen, insbesondere im Hinblick auf

a) deren Zugänglichkeit/Verfügbarkeit,
   Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit an den dafür eingerichteten Arbeitsplätzen verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren.
b) deren Integrität,
   Daten und Anwendungen dürfen nicht unberechtigt gelöscht, zerstört oder manipuliert werden.
c) den Schutz der Daten vor Verlust
   Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern.
d) der Vertraulichkeit
   Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigen.
e) die Einführung, Auswahl, Gestaltung und Änderung von Verfahren
   In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der gemäß § 2 Absatz 3 Zuständige rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.

4. § 4 erhält folgenden Wortlaut:

§ 4
Voraussetzungen für den Einsatz von Informationstechnik

(1) Wesentliche Entscheidungen auf dem Gebiet der IT sind vor allem:

a) der Aufbau neuer IT-Infrastrukturen,
b) der Einsatz von Betriebssystemen,
c) der Einsatz von Anwendungsprogrammen,
d) der Einsatz freigabepflichtiger Anwendungsprogramme,
e) die Nutzung von Kommunikationstechnik.

(2) Mindestvoraussetzungen für den Einsatz von IT sind, dass

a) ein Anforderungsprofil und eine Dokumentation vorliegen,
b) die datenschutzrechtlichen Voraussetzungen eingehalten werden,
c) die Systeme vor ihrem Einsatz getestet wurden und
d) die erforderlichen Lizenzen vorhanden sind.

(3) Für den dienstlichen Datenaustausch ist der Einsatz von einheitlicher Software und IT-Strukturen in vergleichbaren Einsatzbereichen anzustreben.

(4) Bei Anwendungsprogrammen, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, bestehen keine datenschutzrechtlichen Bedenken, wenn

a) dies unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit festgestellt wird,
b) die Rechte Betroffener auf Auskunft, Berichtigung, Löschung und Sperrung ihrer personenbezogener Daten nach Maßgabe des DSG-EKD gewährleistet sind,
c) sie nach dem EKD-Recht (§§ 21 und 21a DSG-EKD) freigegeben worden sind,
d) erforderliche technische und organisatorische Datenschutzmaßnahmen unter Berücksichtigung des IT-Sicherheitskonzeptes, des Schutzbedarfs und der Anforderungen der Anlage zu § 9 Absatz 1 DSG-EKD vorliegen.

5. § 5 erhält folgenden Wortlaut:

§ 5
Nutzung von IT-Geräten

(1) Für die mit der IT verarbeiteten Daten sind dienstliche IT-Geräte zu nutzen, die einheitlichen Standards entsprechen.

(2) In Ausnahmefällen kann der Landeskirchenrat private Geräte zur Nutzung zulassen, wenn durch Vereinbarung insbesondere sichergestellt ist, dass
eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten vorhanden ist,
das kirchliche Datenschutzrecht Anwendung findet,
technische und organisatorische Maßnahmen zur IT-Sicherheit und zum Datenschutz vorhanden sind,
ein regelmäßiger und insbesondere aktueller Schutz vor Viren und anderen Schadprogrammen gewährleistet ist,
die Haftung ausgeschlossen wird, wenn in Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.

(3) Über die Nutzung von dienstlichen und privaten Geräten, die für dienstliche Zwecke genutzt und auf denen personenbezogene Daten gespeichert werden, führt der Landeskirchenrat ein Verzeichnis.

(4) Die Zulassung privater Geräte zur Nutzung ist zu widerrufen, wenn ein Verstoß gegen Absatz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT-Geräte gefährdet oder beeinträchtigt wird.

6. § 6 erhält folgenden Wortlaut:

§ 6
Schulungs- und Fortbildungsmöglichkeiten

In der Landeskirche sind angemessene Schulungs- und Fortbildungsmöglichkeiten für den qualifizierten Umgang mit den Anwendungsprogrammen zu ermöglichen, die zentral von der Landeskirche vorgegeben werden.

7. § 7 erhält folgenden Wortlaut:

§ 7
IT-Sicherheitsbeauftragter

(1) Zur Wahrnehmung der IT-Sicherheit hat der Landeskirchenrat einen für die gesamte Landeskirche zuständigen IT-Sicherheitsbeauftragten und dessen Stellvertretenden zu bestellen.

(2) Zu Beauftragten dürfen nur Personen bestellt werden, die zur Erfüllung ihrer Aufgaben die erforderliche Fachkunde und Zuverlässigkeit besitzen.

(3) Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es insbesondere:
a) bei den IT-Sicherheitsprozess betreffenden Aufgaben mitzuwirken,
b) die Erstellung und Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren,
c) Regelungen zur IT-Sicherheit vorzuschlagen,
d) die Realisierung von Sicherheitsmaßnahmen zu empfehlen und zu überprüfen,
e) IT-Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen,
f) IT-Schulungsmaßnahmen zu initiieren und zu koordinieren,
g) dem Leitungsorgan der kirchlichen Stelle auf Anforderung über den Stand der IT-Sicherheit zu berichten,
h) mit den nach § 2 Absatz 3 Zuständigen zusammenzuarbeiten.

(4) Der IT-Sicherheitsbeauftragte ist unverzüglich über IT-Sicherheitsvorfälle zu informieren. Dieser informiert bei Gefahr im Verzug unverzüglich das zuständige Leitungsorgan und den Beauftragten für Datenschutz. Ist der IT-Sicherheitsbeauftragte nicht erreichbar, ist unverzüglich der Stellvertretende zu informieren.

8. § 8 erhält folgenden Wortlaut:

§ 8
Einhaltung der IT-Sicherheit

(1) Der Landeskirchenrat ist für die Einhaltung der IT-Sicherheit einschließlich der Umsetzung des IT-Sicherheitskonzeptes auf landeskirchlicher sowie auf kirchenkreislicher

Ebene verantwortlich. Der Gemeindekirchenrat ist für die Umsetzung auf kirchengemeindlicher Ebene verantwortlich, das Leitungsorgan der weiteren kirchlichen Dienststelle jeweils für deren Bereich.

(2) Die aufsichtsführenden Stellen oder Personen überwachen die Einhaltung der IT-Sicherheit. Hierfür kann der IT-Sicherheitsbeauftragte beauftragt werden.

(3) Bei Verstößen gegen die IT-Sicherheit sind geeignete Maßnahmen und gegebenenfalls Regelungen zur Gefahrenintervention zu ergreifen. Neben den arbeitsrechtlichen und datenschutzrechtlichen Konsequenzen sind folgende Sanktionen möglich:

a) die Beanstandung bei geringfügigen individuellen Verstößen,
b) die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen,
c) bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen,
d) die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage bis der Nachweis über die die Beseitigung des Missstandes erbracht ist,
e) Entzug der IT-relevanten Tätigkeit bei Ehrenamtlichen.

(4) Maßnahmen der oder des Beauftragten für Datenschutz nach § 20 DSG-EKD bleiben unberührt.

§ 2

Der Landeskirchenrat wird gebeten, eine Neufassung der IT-Sicherheitsordnung in der vom 1. Juli 2015 an geltenden Fassung bekannt zu machen.

§ 3

Dieses Kirchengesetz tritt am 1. Juli 2015 in Kraft.

Andreas Schindler
Präses der Landessynode

Begründung:
Die von der Arbeitsgruppe IT-Sicherheit erarbeiteten Novellierungsvorschläge für die Änderung der IT-Sicherheitsordnung werden der Landessynode zur Beschlussfassung vorgelegt.
Die Landessynode hat die Wirksamkeit der IT-Sicherheitsordnung in der Ursprungsfassung in Kraft gesetzt. Der Text ist abrufbar unter http://www.landeskirche-anhalts.de/service/rechtssammlung/it-sicherheitsordnung und veröffentlicht im KABl 2013 S.3, 38. Da sich die Anforderungen an die IT-Sicherheitsordnung seit 2013 verändert haben, hat die im Anschluss an die Herbsttagung der Landessynode 2013 vom Landeskirchenrat eingesetzte Arbeitsgruppe (Frau Silvia Schmidt (Vorsitzende), Herr Stephan Lux, Frau Ute Krause (Mitglied der Landessynode), Herr Michael Tiefenau (Mitglied der Landessynode), Herr Daniel Piasecki (Mitglied der EKD-Arbeitsgruppe IT-Sicherheit), Frau Annette Heß (Datenschutzbeauftragte der Landeskirche) und OKR Dr. Rainer Rausch Änderungsvorschläge unterbreitet. Der Landeskirchenrat hat in seiner Sitzung vom 20. Januar 2015 beschlossen, die erarbeiteten Änderungen der IT-Sicherheitsordnung zur Einleitung des Gesetzgebungsverfahrens der Kirchenleitung als Vorlage des Landeskirchenrates vorgelegt werden. Der Rechts-und Verfassungsausschuss hat die Änderungen beraten und beschlossen, diese Beratungen als erste Lesung zu werten.

Synopse:

Ursprüngliche Fassung vom 8. Juli 2013	**Vorgeschlagene Änderungen**
Präambel	
Der Gebrauch von Computern und Netzen ist für die haupt-, neben- und ehrenamtlichen Mitarbeitenden in der Evangelischen Landeskirche Anhalts zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtert der Computer viele Tätigkeiten und manche Arbeiten wären ohne den Einsatz von Computern gar nicht mehr denkbar. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer verletzen. Daher haben alle Nutzer sorgfältig und verantwortungsvoll unter Einhaltung der rechtlichen Vorschriften Computer und Netze zu nutzen.	*Die Präambel erhält folgenden Wortlaut:* Der Gebrauch von Computern und Netzen ist für die haupt-, neben- und ehrenamtlichen Mitarbeitenden in der Evangelischen Landeskirche Anhalts zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtert der Computer viele Tätigkeiten und manche Arbeiten wären ohne den Einsatz von Computern gar nicht mehr denkbar. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer verletzen. Daher haben alle Nutzer sorgfältig und verantwortungsvoll unter Einhaltung der rechtlichen Vorschriften Computer und Netze zu nutzen.
In dieser Vorschrift wird aufgezeigt, welche Mindeststandards für den Betrieb eines Computers bzw. eines Netzes verbindlich sind und welche Konsequenzen bei Nichteinhaltung der IT-Sicherheitsordnung gezogen werden. Zweck der IT-Sicherheitsordnung ist es, diese Themenkreise zu formalisieren und allen Benutzern eine einheitliche Grundlage zu bieten, anhand derer entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind.	In dieser Vorschrift wird aufgezeigt, welche Mindeststandards für den Betrieb eines Computers bzw. eines Netzes verbindlich sind und welche Konsequenzen bei Nichteinhaltung der IT-Sicherheitsordnung gezogen werden. Zweck der IT-Sicherheitsordnung ist es, diese Themenkreise zu formalisieren und allen Benutzern eine einheitliche Grundlage zu bieten, anhand derer entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind.
Die Informationssicherheit ist systematisch und umfassend an die technischen und rechtlichen Entwicklungen anzupassen, damit eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten erreicht wird. Dabei sind die umgesetzten Lösungen praxistauglich und ausreichend komfortabel zu gestalten, damit sie von	Die Informationssicherheit ist systematisch und umfassend an die technischen und rechtlichen Entwicklungen anzupassen, damit eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten erreicht wird. Dabei sind die umgesetzten Lösungen praxistauglich und ausreichend komfortabel zu gestalten, damit sie von den Mitarbeitenden auch in

den Mitarbeitenden auch in der täglichen Arbeit nicht als belastend, sondern als sinnvoll akzeptiert werden. Auf Grund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die IT-Sicherheitsordnung soll das Erkennen von Sicherheitsproblemen beschleunigt werden, um Schaden zu vermeiden. Die IT-Sicherheitsordnung soll als Richtschnur für das eigene Handeln, sowie für das Beurteilen des Handelns der anderen dienen.	der täglichen Arbeit nicht als belastend, sondern als sinnvoll akzeptiert werden. Auf Grund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die IT-Sicherheitsordnung soll für IT-Sicherheit sensibilisiert werden. Die IT-Sicherheitsordnung soll als Richtschnur für das eigene Handeln, sowie für das Beurteilen des Handelns der Anderen dienen.
§ 2 IT-Sicherheitsstandard	
(2)°Jede kirchliche Stelle hat das vom Landeskirchenrat erstellte aktuelle IT-Sicherheitskonzept der Landeskirche umzusetzen. Die Landeskirche hat das IT-Sicherheitskonzept regelmäßig zu aktualisieren. (3)°Bei der Erstellung und der regelmäßigen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, ist der Betriebsbeauftragte für den Datenschutz frühzeitig zu beteiligen. (4)°Der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard orientiert sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)°zur Informationssicherheit und zum IT-Grundschutz. Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen Gefährdungen von innen und außen enthalten. Die IT-	*§ 2 Absatz 2 erhält folgenden Wortlaut:* (2) Jede kirchliche Stelle im Sinne des § 1 Absatz 2 Satz 1 des Datenschutzgesetzes der EKD (DSG-EKD) hat das vom Landeskirchenrat erstellte aktuelle IT-Sicherheitskonzept der Landeskirche umzusetzen. Der Landeskirchenrat hat das IT-Sicherheitskonzept regelmäßig zu aktualisieren. *§2 Absatz 3 erhält folgenden Wortlaut:* (3) Bei der Erstellung und der regelmäßigen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, ist soweit vorhanden, der Betriebsbeauftragte für den Datenschutz frühzeitig zu beteiligen. Anderenfalls ist der landeskirchliche Beauftragte nach § 18 DSG-EKD zu beteiligen. *§ 2 Absatz 4 erhält folgenden Wortlaut:* (4) Der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard orientiert sich an den jeweiligen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz oder einem vergleichbaren Standard. Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen

Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Schutzbedarf der Daten und der IT-Systeme stehen. (5)°Der Landeskirchenrat stellt Muster-IT-Sicherheitskonzepte zur Verfügung, die die Mindestanforderungen der IT-Sicherheit unter Berücksichtigung der örtlichen Gegebenheiten darstellen.	Gefährdungen von innen und außen enthalten. Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Schutzbedarf der Daten und der IT-Systeme stehen. *§ 2 Absatz 5 erhält folgenden Wortlaut:* (5) Die Evangelische Landeskirche Anhalts führt für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit, für die das DSG-EKD gilt (gemäß § 1 Absatz 2 Sätze 3 und 4 DSG-EKD). Der Landeskirchenrat stellt Muster-IT-Sicherheitskonzepte insbesondere für die Landeskirche, die Kirchengemeinden und die im Satz 1 erwähnten Werke und Einrichtungen zur Verfügung, die die Mindestanforderungen der IT-Sicherheit unter Berücksichtigung der örtlichen und sachlichen Gegebenheiten darstellen und einzuhalten sind.
§ 3 IT-Sicherheitsziele	
(2)°Die mit der Informationstechnik erhobenen, verarbeiteten, übertragenen und gespeicherten Daten sind zu schützen, insbesondere im Hinblick auf 1. deren Zugänglichkeit/Verfügbarkeit Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit von jedem Arbeitsplatz bei Bedarf verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren. 2. deren Integrität Daten und Anwendungen dürfen nicht unberechtigt gelöscht, zerstört oder manipuliert werden.	*§ 3 Absatz 2 erhält folgenden Wortlaut*: (2) Die mit der Informationstechnik erhobenen, verarbeiteten und genutzten Daten sind zu schützen, insbesondere im Hinblick auf a) deren Zugänglichkeit/Verfügbarkeit Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit an den dafür vorgesehenen Arbeitsplätzen verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren. b) deren Integrität Daten und Anwendungen dürfen nicht

3. den Schutz der Daten vor Verlust Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern. 4. Vertraulichkeit Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigten. 5. die Einführung, Auswahl, Gestaltung und Änderung von Verfahren In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der zuständige kirchliche Datenschutzbeauftragte rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.	unberechtigt gelöscht, zerstört oder manipuliert werden. c) den Schutz der Daten vor Verlust Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern. d) Vertraulichkeit Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigen. e) die Einführung, Auswahl, Gestaltung und Änderung von Verfahren In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der gemäß § 2 Absatz 3 Zuständige rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.
§ 4 Voraussetzungen für den Einsatz von Informationstechnik	
(1) Wesentliche Entscheidungen auf dem Gebiet der IT sind vor allem: - der Aufbau neuer IT-Infrastrukturen, - der Wechsel zu anderen Betriebssystemen, - der Einsatz neuer Anwendungsprogramme, - der Einsatz freigabepflichtiger Programme, - die Nutzung neuer Kommunikationstechnik. (2)°Mindestvoraussetzungen für den Einsatz von IT sind, dass 1.°ein Anforderungsprofil und eine Dokumentation vorliegen, 2.°die datenschutzrechtlichen Voraussetzungen vorliegen, 3.°diese getestet worden ist und	*§ 4 Absatz 1 erhält folgenden Wortlaut:* (1) Wesentliche Entscheidungen auf dem Gebiet der IT sind vor allem: a) der Aufbau neuer IT-Infrastrukturen, b) der Einsatz von Betriebssystemen, c) der Einsatz von Anwendungsprogrammen, d) der Einsatz freigabepflichtiger Anwendungsprogramme, e) die Nutzung von Kommunikationstechnik. *§ 4 Absatz 2 erhält folgenden Wortlaut:* (2) Mindestvoraussetzungen für den Einsatz von IT sind, dass a) ein Anforderungsprofil und eine Dokumentation vorliegen, b) die datenschutzrechtlichen Voraussetzungen eingehalten werden, c) die Systeme vor ihrem Einsatz

4.°die erforderlichen Lizenzen vorhanden sind.	getestet wurden und d) die erforderlichen Lizenzen vorhanden sind.
(3) Die Anforderungen an die Einheitlichkeit betreffen den Einsatz von Programmen in vergleichbaren Einsatzbereichen und die IT – Struktur für den dienstlichen Datenaustausch.	*§ 4 Absatz 3 erhält folgenden Wortlaut:* (3) Für den dienstlichen Datenaustausch ist der Einsatz von einheitlicher Software und IT-Strukturen in vergleichbaren Einsatzbereichen anzustreben.
(4)°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, - die rechtliche Zulässigkeit der Erhebung, Speicherung und Übermittlungen der personenbezogenen Daten unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit festgestellt wird, - den Auskunftsrechten nach Maßgabe des Datenschutzgesetzes der EKD (DSG-EKD)°entsprochen werden kann, - die Berichtigung, Löschung und Sperrung personenbezogener Daten nach Maßgabe des Datenschutzgesetzes der EKD (DSG-EKD)°möglich ist, - bei Speicherung dienstlicher Daten ausreichende organisatorische und technische Maßnahmen entsprechend des IT- Sicherheitskonzeptes einen möglichen unberechtigten Zugriff ausschließen, - ausreichende technische und organisatorische Datenschutzmaßnahmen unter Berücksichtigung des Schutzbedarfs und der Anforderungen der Anlage zu § 9 Absatz 1 DSG-EKD vorliegen.	*§ 4 Absatz 4 erhält folgenden Wortlaut:* (4) Bei Anwendungsprogrammen, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, bestehen keine datenschutzrechtlichen Bedenken, wenn a) dies unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit festgestellt wird, b) die Rechte Betroffener auf Auskunft, Berichtigung, Löschung und Sperrung ihrer personenbezogener Daten nach Maßgabe des DSG-EKD gewährleistet sind, c) sie nach dem EKD-Recht (§§ 21 und 21a DSG-EKD) freigegeben worden sind, d) erforderliche technische und organisatorische Datenschutzmaßnahmen unter Berücksichtigung des IT-Sicherheitskonzeptes, des Schutzbedarfs und der Anforderungen der Anlage zu § 9 Absatz 1 DSG-EKD vorliegen.

§ 5 Nutzung von IT-Geräten	
(1)°Für die mit der IT verarbeiteten Daten sind dienstliche IT-Geräte zu nutzen.	*§ 5 Absatz 1 erhält folgenden Wortlaut:* (1) Für die mit der IT verarbeiteten Daten sind dienstliche IT-Geräte zu nutzen, die einheitlichen Standards entsprechen.
(2)°In Ausnahmefällen kann der Landeskirchenrat private Geräte zur Nutzung zulassen, wenn durch Vereinbarung insbesondere sichergestellt ist, dass a)°eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten vorhanden ist, b)°das kirchliche Datenschutzrecht Anwendung findet, c)°technische und organisatorische Maßnahmen zur IT-Sicherheit und zum Datenschutz vorhanden sind, d)°ein regelmäßiger und insbesondere aktueller Schutz vor Viren und anderen schädigenden Programmen gewährleistet ist, e)°die Haftung ausgeschlossen wird, wenn in Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.	*§ 5 Absatz 2 erhält folgenden Wortlaut:* (2) In Ausnahmefällen kann der Landeskirchenrat private Geräte zur Nutzung zulassen, wenn durch Vereinbarung insbesondere sichergestellt ist, dass a) eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten vorhanden ist, b) das kirchliche Datenschutzrecht Anwendung findet, c) technische und organisatorische Maßnahmen zur IT-Sicherheit und zum Datenschutz vorhanden sind, d) ein regelmäßiger und insbesondere aktueller Schutz vor Viren und anderen Schadprogrammen gewährleistet ist, e) die Haftung ausgeschlossen wird, wenn in Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.
(3)°Die Zulassung privater Geräte zur Nutzung ist zu widerrufen, wenn ein Verstoß gegen Absatz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT-Geräte gefährdet oder beeinträchtigt wird.	*§ 5 Absatz 3 erhält folgenden Wortlaut:* (3) Über die Nutzung von dienstlichen und privaten Geräten, die für dienstliche Zwecke genutzt und auf denen personenbezogene Daten gespeichert werden, führt der Landeskirchenrat ein Verzeichnis. *§ 5 Absatz 4 erhält folgenden Wortlaut:* (4) Die Zulassung privater Geräte zur Nutzung ist zu widerrufen, wenn ein Verstoß gegen Absatz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT-Geräte gefährdet oder beeinträchtigt wird.

§ 6 Schulungs- und Fortbildungsmöglichkeiten	
In der Landeskirche sind angemessene Schulungs- und Fortbildungsmöglichkeiten für den qualifizierten Umgang mit IT zu ermöglichen.	*§ 6 erhält folgenden Wortlaut:* In der Landeskirche sind angemessene Schulungs- und Fortbildungsmöglichkeiten für den qualifizierten Umgang mit den Anwendungsprogrammen zu ermöglichen, die zentral von der Landeskirche vorgegeben werden.
§ 7 IT-Sicherheitsbeauftragter	
(1)°Zur Wahrnehmung der IT-Sicherheit hat der Landeskirchenrat einen IT-Sicherheitsbeauftragten zu bestellen.	*§ 7 Absatz 1erhält folgenden Wortlaut:* (1) Zur Wahrnehmung der IT-Sicherheit hat der Landeskirchenrat einen für die gesamte Landeskirche zuständigen IT-Sicherheitsbeauftragten und dessen Stellvertretenden zu bestellen.
(2)°Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es insbesondere: a)°bei den IT-Sicherheitsprozess betreffenden Aufgaben mitzuwirken, b)°die Erstellung und Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren, c)°Regelungen zur IT-Sicherheit vorzuschlagen, d)°die Realisierung von Sicherheitsmaßnahmen zu empfehlen und zu überprüfen, e)°Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen, f)°Schulungsmaßnahmen zu initiieren und zu koordinieren, g)°dem Leitungsorgan der kirchlichen Stelle auf Anforderung über den Stand der IT- Sicherheit zu berichten, h)°mit den Betriebsbeauftragten für den Datenschutz zusammenzuarbeiten.	*§ 7 Absatz 2erhält folgenden Wortlaut* (2) Zu Beauftragten dürfen nur Personen bestellt werden, die zur Erfüllung ihrer Aufgaben die erforderliche Fachkunde und Zuverlässigkeit besitzen.
(3)°Der IT-Sicherheitsbeauftragte ist über Sicherheitsvorfälle zu informieren.	*§ 7 Absatz 3erhält folgenden Wortlaut* (3) Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es insbesondere: a) bei den IT-Sicherheitsprozess

	betreffenden Aufgaben mitzuwirken, b) die Erstellung und Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren, c) Regelungen zur IT-Sicherheit vorzuschlagen, d) die Realisierung von Sicherheitsmaßnahmen zu empfehlen und zu überprüfen, e) IT-Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen, f) IT-Schulungsmaßnahmen zu initiieren und zu koordinieren, g) dem Leitungsorgan der kirchlichen Stelle auf Anforderung über den Stand der IT-Sicherheit zu berichten, h) mit den nach § 2 Absatz 3 Zuständigen zusammenzuarbeiten. (4) Der IT-Sicherheitsbeauftragte ist unverzüglich über IT-Sicherheitsvorfälle zu informieren. Dieser informiert bei Gefahr im Verzug unverzüglich das zuständige Leitungsorgan und den Beauftragten für Datenschutz. Ist der IT-Sicherheitsbeauftragte nicht erreichbar, ist unverzüglich der Stellvertretende zu informieren.
§ 8 Einhaltung der IT-Sicherheit	
(1)°Zur Wahrnehmung der IT-Sicherheit hat der Landeskirchenrat einen IT-Sicherheitsbeauftragten zu bestellen.	*§ 8 Absatz 1 erhält folgenden Wortlaut:* (1) Der Landeskirchenrat ist für die Einhaltung der IT-Sicherheit einschließlich der Umsetzung des IT-Sicherheitskonzeptes auf landeskirchlicher sowie auf kirchenkreislicher Ebene verantwortlich. Der Gemeindekirchenrat ist für die Umsetzung auf kirchengemeindlicher Ebene verantwortlich, das Leitungsorgan der weiteren kirchlichen Dienststelle jeweils für deren Bereich.
(2) Die aufsichtsführenden Stellen oder Personen überwachen die	*§ 8 Absatz 2 erhält folgenden Wortlaut:* (2) Die aufsichtsführenden Stellen oder Personen überwachen die Einhaltung der

Einhaltung der IT-Sicherheit. Hierfür kann der/die IT-Sicherheitsbeauftragte beauftragt werden. (3) Bei Verstößen gegen die IT-Sicherheit sind geeignete Maßnahmen zu ergreifen. Neben den arbeitsrechtlichen und datenschutzrechtlichen Konsequenzen sind folgende Sanktionen möglich: 1. die Beanstandung bei geringfügigen individuellen Verstößen, 2. die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen, 3. bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen, 4. Regelungen zur Gefahrenintervention, 5. die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage bis der Nachweis über die die Beseitigung des Missstandes erbracht ist. 6. Entzug der IT-relevanten Tätigkeit bei Ehrenamtlichen.	IT-Sicherheit. Hierfür kann der IT-Sicherheitsbeauftragte beauftragt werden. *§ 8 Absatz 3 erhält folgenden Wortlaut:* (3) Bei Verstößen gegen die IT-Sicherheit sind geeignete Maßnahmen und gegebenenfalls Regelungen zur Gefahrenintervention zu ergreifen. Neben den arbeitsrechtlichen und datenschutzrechtlichen Konsequenzen sind folgende Sanktionen möglich: a) die Beanstandung bei geringfügigen individuellen Verstößen, b) die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen, c) bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen, d) die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage bis der Nachweis über die die Beseitigung des Missstandes erbracht ist. e) der Entzug der IT-relevanten Tätigkeit bei Ehrenamtlichen. (4) Maßnahmen der oder des Beauftragten für Datenschutz nach § 20 DSG-EKD bleiben unberührt.

Vollständige Fassung im Falle der Verabschiedung als Kirchengesetz

Ordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik (IT)
(IT-Sicherheitsordnung)

vom … April 2015

Die Kirchenleitung hat nach Maßgabe des gemäß § 59 Absatz 1 Buchstabe b Kirchenverfassung auf Grund von § 9 Absatz 2 Satz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993 (ABl. EKD S. 505) in der Fassung der Neubekanntmachung vom 1. Januar 2013 (ABl. EKD 2013 S. 2 und S. 34) die folgende gesetzesvertretende Verordnung beschlossen, die durch Kirchengesetz vom … April 2015 geändert worden ist:

Inhaltsverzeichnis

Präambel

Der Gebrauch von Computern und Netzen ist für die haupt-, neben- und ehrenamtlichen Mitarbeitenden in der Evangelischen Landeskirche Anhalts zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtert der Computer viele Tätigkeiten und manche Arbeiten wären ohne den Einsatz von Computern gar nicht mehr denkbar. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer verletzen. Daher haben alle Nutzer sorgfältig und verantwortungsvoll unter Einhaltung der rechtlichen Vorschriften Computer und Netze zu nutzen.

In dieser Vorschrift wird aufgezeigt, welche Mindeststandards für den Betrieb eines Computers bzw. eines Netzes verbindlich sind und welche Konsequenzen bei Nichteinhaltung der IT-Sicherheitsordnung gezogen werden. Zweck der IT-Sicherheitsordnung ist es, diese Themenkreise zu formalisieren und allen Benutzern eine

einheitliche Grundlage zu bieten, anhand derer entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind.

Die Informationssicherheit ist systematisch und umfassend an die technischen und rechtlichen Entwicklungen anzupassen, damit eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten erreicht wird. Dabei sind die umgesetzten Lösungen praxistauglich und ausreichend komfortabel zu gestalten, damit sie von den Mitarbeitenden auch in der täglichen Arbeit nicht als belastend, sondern als sinnvoll akzeptiert werden.

Auf Grund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die IT-Sicherheitsordnung soll für IT-Sicherheit sensibilisiert werden. Die IT-Sicherheitsordnung soll als Richtschnur für das eigene Handeln, sowie für das Beurteilen des Handelns der Anderen dienen.

§ 1
Geltungsbereich

Die IT- Sicherheitsordnung ist verbindlich für sämtliche haupt-, neben- und ehrenamtlich Mitarbeitende in der Evangelischen Landeskirche Anhalts sowie für Dritte, mit denen die Benutzung von Computern und Netzen von kirchlichen Einrichtungen vereinbart worden ist.

§ 2
IT-Sicherheitsstandard

(1) Die mit der Informationstechnik (IT) erhobenen und verarbeiteten Daten sind insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes zu schützen (IT-Sicherheit), um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

(2) Jede kirchliche Stelle im Sinne des § 1 Absatz 2 Satz 1 des Datenschutzgesetzes der EKD (DSG-EKD) hat das vom Landeskirchenrat erstellte aktuelle IT-Sicherheitskonzept der Landeskirche umzusetzen. Der Landeskirchenrat hat das IT-Sicherheitskonzept regelmäßig zu aktualisieren.

(3) Bei der Erstellung und der regelmäßigen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, ist soweit vorhanden, der Betriebsbeauftragte für den Datenschutz frühzeitig zu beteiligen. Anderenfalls ist der landeskirchliche Beauftragte nach § 18 DSG-EKD zu beteiligen.

(4) Der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard orientiert sich an den jeweiligen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz oder einem vergleichbaren Standard. Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen Gefährdungen von innen und außen enthalten. Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Schutzbedarf der Daten und der IT-Systeme stehen.

(5) Die Evangelische Landeskirche Anhalts führt für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit, für die das DSG-EKD gilt (gemäß § 1 Absatz 2 Sätze 3 und 4 DSG-EKD). Der Landeskirchenrat stellt Muster-IT-Sicherheitskonzepte insbesondere für die Landeskirche, die Kirchengemeinden und die im Satz 1 erwähnten Werke und Einrichtungen zur Verfügung, die die Mindestanforderungen der IT-Sicherheit unter Berücksichtigung der örtlichen und sachlichen Gegebenheiten darstellen und einzuhalten sind.

§ 3
IT-Sicherheitsziele

(1) Die IT-Sicherheitsordnung definiert grundlegende Ziele einer IT-Sicherheit und legt Verantwortlichkeiten sowie Rahmenbedingungen für die Umsetzung des IT-Sicherheitsstandards fest.

(2) Die mit der Informationstechnik erhobenen, verarbeiteten und genutzten Daten sind zu schützen, insbesondere im Hinblick auf

a) deren Zugänglichkeit/Verfügbarkeit,
   Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit an den dafür eingerichteten Arbeitsplätzen verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren.
b) deren Integrität,
   Daten und Anwendungen dürfen nicht unberechtigt gelöscht, zerstört oder manipuliert werden.
c) den Schutz der Daten vor Verlust,
   Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern.
d) der Vertraulichkeit
   Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigen.
e) die Einführung, Auswahl, Gestaltung und Änderung von Verfahren
   In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der gemäß § 2 Absatz 3 Zuständige rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.

§ 4
Voraussetzungen für den Einsatz von Informationstechnik

(1) Wesentliche Entscheidungen auf dem Gebiet der IT sind vor allem:

a) der Aufbau neuer IT-Infrastrukturen,
b) der Einsatz von Betriebssystemen,
c) der Einsatz von Anwendungsprogrammen,
d) der Einsatz freigabepflichtiger Anwendungsprogramme,
e) die Nutzung von Kommunikationstechnik.

(2) Mindestvoraussetzungen für den Einsatz von IT sind, dass

a) ein Anforderungsprofil und eine Dokumentation vorliegen,
b) die datenschutzrechtlichen Voraussetzungen eingehalten werden,
c) die Systeme vor ihrem Einsatz getestet wurden und
d) die erforderlichen Lizenzen vorhanden sind.

(3) Für den dienstlichen Datenaustausch ist der Einsatz von einheitlicher Software und IT-Strukturen in vergleichbaren Einsatzbereichen anzustreben.

(4) Bei Anwendungsprogrammen, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, bestehen keine datenschutzrechtlichen Bedenken, wenn

a) dies unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit festgestellt wird,
b) die Rechte Betroffener auf Auskunft, Berichtigung, Löschung und Sperrung ihrer personenbezogener Daten nach Maßgabe des DSG-EKD gewährleistet sind,
c) sie nach dem EKD-Recht (§§ 21 und 21a DSG-EKD) freigegeben worden sind,
d) erforderliche technische und organisatorische Datenschutzmaßnahmen unter Berücksichtigung des IT-Sicherheitskonzeptes, des Schutzbedarfs und der Anforderungen der Anlage zu § 9 Absatz 1 DSG-EKD vorliegen.

§ 5
Nutzung von IT-Geräten

(1) Für die mit der IT verarbeiteten Daten sind dienstliche IT-Geräte zu nutzen, die einheitlichen Standards entsprechen.

(2) In Ausnahmefällen kann der Landeskirchenrat private Geräte zur Nutzung zulassen, wenn durch Vereinbarung insbesondere sichergestellt ist, dass

a) eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten vorhanden ist,
b) das kirchliche Datenschutzrecht Anwendung findet,
c) technische und organisatorische Maßnahmen zur IT-Sicherheit und zum Datenschutz vorhanden sind,
d) ein regelmäßiger und insbesondere aktueller Schutz vor Viren und anderen Schadprogrammen gewährleistet ist,

e) die Haftung ausgeschlossen wird, wenn in Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.

(3) Über die Nutzung von dienstlichen und privaten Geräten, die für dienstliche Zwecke genutzt und auf denen personenbezogene Daten gespeichert werden, führt der Landeskirchenrat ein Verzeichnis.

4) Die Zulassung privater Geräte zur Nutzung ist zu widerrufen, wenn ein Verstoß gegen Absatz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT-Geräte gefährdet oder beeinträchtigt wird.

§ 6
Schulungs- und Fortbildungsmöglichkeiten

In der Landeskirche sind angemessene Schulungs- und Fortbildungsmöglichkeiten für den qualifizierten Umgang mit den Anwendungsprogrammen zu ermöglichen, die zentral von der Landeskirche vorgegeben werden.

§ 7
IT-Sicherheitsbeauftragter

(1) Zur Wahrnehmung der IT-Sicherheit hat der Landeskirchenrat einen für die gesamte Landeskirche zuständigen IT-Sicherheitsbeauftragten und dessen Stellvertretenden zu bestellen.

(2) Zu Beauftragten dürfen nur Personen bestellt werden, die zur Erfüllung ihrer Aufgaben die erforderliche Fachkunde und Zuverlässigkeit besitzen.

(3) Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es insbesondere:

a) bei den IT-Sicherheitsprozess betreffenden Aufgaben mitzuwirken,
b) die Erstellung und Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren,
c) Regelungen zur IT-Sicherheit vorzuschlagen,
d) die Realisierung von Sicherheitsmaßnahmen zu empfehlen und zu überprüfen,
e) IT-Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen,
f) IT-Schulungsmaßnahmen zu initiieren und zu koordinieren,
g) dem Leitungsorgan der kirchlichen Stelle auf Anforderung über den Stand der IT-Sicherheit zu berichten,
h) mit den nach § 2 Absatz 3 Zuständigen zusammenzuarbeiten

(4) Der IT-Sicherheitsbeauftragte ist unverzüglich über IT-Sicherheitsvorfälle zu informieren. Dieser informiert bei Gefahr im Verzug unverzüglich das zuständige Leitungsorgan und den Beauftragten für Datenschutz. Ist der IT-Sicherheitsbeauftragte nicht erreichbar, ist unverzüglich der Stellvertretende zu informieren.

§ 8
Einhaltung der IT-Sicherheit

(1) Der Landeskirchenrat ist für die Einhaltung der IT-Sicherheit einschließlich der Umsetzung des IT-Sicherheitskonzeptes auf landeskirchlicher sowie auf kirchenkreislicher Ebene verantwortlich. Der Gemeindekirchenrat ist für die Umsetzung auf kirchengemeindlicher Ebene verantwortlich, das Leitungsorgan der weiteren kirchlichen Dienststelle jeweils für deren Bereich.

(2) Die aufsichtsführenden Stellen oder Personen überwachen die Einhaltung der IT-Sicherheit. Hierfür kann der IT-Sicherheitsbeauftragte beauftragt werden.

(3) Bei Verstößen gegen die IT-Sicherheit sind geeignete Maßnahmen und gegebenenfalls Regelungen zur Gefahrenintervention zu ergreifen. Neben den arbeitsrechtlichen und datenschutzrechtlichen Konsequenzen sind folgende Sanktionen möglich:

a) die Beanstandung bei geringfügigen individuellen Verstößen,
b) die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen,
c) bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen,
d) die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage bis der Nachweis über die die Beseitigung des Missstandes erbracht ist,
e) Entzug der IT-relevanten Tätigkeit bei Ehrenamtlichen.

(4) Maßnahmen der oder des Beauftragten für Datenschutz nach § 20 DSG-EKD bleiben unberührt.

§ 9
Ausführungsbestimmungen

Der Landeskirchenrat kann Durchführungsbestimmungen beschließen.

§ 10
Inkrafttreten

Diese Regelungen treten am 1. Juli 2013 in Kraft. Die Neufasssung tritt am 1. Juli 2015 in Kraft.