Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD)

Vom 29. Mai 2015

(ABl. EKD S. 146)

Der Rat der Evangelischen Kirche in Deutschland hat auf Grund des § 9 Absatz 2 Satz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) in der Fassung der Neubekanntmachung vom 1. Januar 2013 (ABl. EKD 2013, S. 2 und S. 34) mit Zustimmung der Kirchenkonferenz folgende Rechtsverordnung erlassen:

§ 1
IT-Sicherheit

(1) Die mit der Informationstechnik (IT) erhobenen oder 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) $_1$Zur Umsetzung der IT-Sicherheit haben die Evangelische Kirche in Deutschland, ihre Gliedkirchen und ihre gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen ohne Rücksicht auf deren Rechtsform und rechtsfähige evangelische Stiftungen des bürgerlichen Rechts (kirchliche Stellen) sicherzustellen, dass ein IT-Sicherheitskonzept erstellt und kontinuierlich fortgeschrieben wird. $_2$Dabei ist den unterschiedlichen Gegebenheiten der kirchlichen Stellen Rechnung zu tragen.

(3) $_1$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. $_2$Andere vergleichbare Sicherheitsstandards können zu Grunde gelegt werden. $_3$Das IT-Sicherheitskonzept muss den Schutzbedarf der Daten, die Art der eingesetzten IT und die örtlichen Gegebenheiten der jeweiligen kirchlichen Stelle berücksichtigen.

(4) Die Evangelische Kirche in Deutschland stellt Muster-IT-Sicherheitskonzepte nach Maßgabe des Absatzes 3 zur Verfügung.

§ 2
Einsatz von IT

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

1. ein Anforderungsprofil und eine Dokumentation vorliegen,
2. die datenschutzrechtlichen Anforderungen eingehalten werden,
3. die Systeme vor ihrem Einsatz getestet wurden.

(2) [1]Für die mit IT-Sicherheit verarbeiteten Daten soll dienstliche IT genutzt werden. [2]Private IT-Geräte dürfen zugelassen werden, wenn durch Vereinbarung insbesondere sichergestellt ist, dass

1. eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten gegeben ist,
2. das kirchliche Datenschutzrecht Anwendung findet,
3. die notwendigen technischen und organisatorischen Maßnahmen zur IT-Sicherheit und zum Datenschutz getroffen und Regelungen zur Verantwortung vereinbart worden sind und
4. eine Haftung des Dienstgebers ausgeschlossen ist, wenn im Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.

[3]Die Zulassung ist zu widerrufen, wenn ein Verstoß gegen Satz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT gefährdet oder beeinträchtigt wird und andere Maßnahmen nicht zur Behebung ausreichen.

§ 3
Beteiligung

Bei der Erstellung und der kontinuierlichen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, sind Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz frühzeitig zu beteiligen.

§ 4
Einhaltung der IT-Sicherheit

(1) Kirchliche Stellen haben durch angemessene Schulungs- und Fortbildungsmöglichkeiten den qualifizierten Umgang mit IT zu ermöglichen.

(2) [1]Die Verantwortung für die IT-Sicherheit liegt beim Leitungsorgan der jeweiligen kirchlichen Stelle. [2]Die aufsichtführenden Stellen oder Personen überwachen die Einhaltung dieser Verordnung. [3]Bei Verstößen sind geeignete Maßnahmen zu ergreifen. § 5 bleibt unberührt.

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

§ 5
IT-Sicherheitsbeauftragte

(1) [1]Mit der Wahrnehmung der IT-Sicherheit können kirchliche Stellen besondere Personen beauftragen (IT-Sicherheitsbeauftragte). [2]Die Beauftragung kann mehrere kirchliche Stellen umfassen.

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

(3) Zu den Aufgaben der die IT-Sicherheit wahrnehmenden Person zählen insbesondere:

1. den IT-Sicherheitsprozess beratend zu begleiten und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
2. die Erstellung und kontinuierliche Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren,
3. Regelungen zur IT-Sicherheit vorzuschlagen,
4. die Durchführung von IT-Sicherheitsmaßnahmen zu empfehlen und zu überprüfen,
5. IT-Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen
6. IT-Schulungen zu initiieren und zu koordinieren,
7. dem Leitungsorgan der jeweiligen kirchlichen Stelle regelmäßig über den Stand der IT-Sicherheit sowie über ihre Tätigkeiten zu berichten und
8. mit den Betriebsbeauftragten oder den örtlich Beauftragten für den Datenschutz zusammenzuarbeiten.

(4) Die die Aufgaben der IT-Sicherheit wahrnehmende Person ist über IT-Sicherheitsvorfälle zu informieren und informiert bei Gefahr im Verzug unverzüglich das zuständige Leitungsorgan.

§ 6
Durchführungs- und Ergänzungsbestimmungen

(1) Die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse können jeweils für ihren Bereich Durchführungsbestimmungen zu dieser Verordnung und ergänzende Bestimmungen zur IT-Sicherheit erlassen, soweit sie dieser Verordnung nicht widersprechen.

(2) [1]Bestehende Regelungen bleiben unberührt, soweit sie dieser Verordnung nicht widersprechen. [2]Anderenfalls sind diese Regelungen innerhalb eines Jahres anzupassen.

§ 7
Übergangsbestimmungen

Die erstmalige Erstellung des IT-Sicherheitskonzeptes gemäß § 1 Absatz 2 hat in ihren Grundzügen spätestens bis zum 31. Dezember 2015 zu erfolgen und deren vollständige Umsetzung bis zum 31. Dezember 2017.

§ 8
Inkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung[1] in Kraft.

1 Veröffentlicht am 15. Juli 2015; Inkrafttreten am 16. Juli 2015