Verordnung über die Sicherheit beim Einsatz von Informationstechnik (IT) (IT-Sicherheitsverordnung)

Vom 17. März 2011

(GVM 2011 Nr. 1 S. 172)

Auf Grund von § 27 Absatz 2[1] des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)[2] vom 12. November 1993 (ABl. EKD 1993, S. 505) in der Fassung vom 7. November 2002 (ABl. EKD 2002, S. 381)[3] sowie § 12 Absatz 1 Satz 3 der Verfassung der Bremischen Evangelischen Kirche[4] (GVM 1930 Nr. 3 Z. 1) in der Fassung vom 29. November 2006 (GVM 2007 Nr. 1 S. 207) erlässt der Kirchenausschuss der Bremischen Evangelischen Kirche folgende Verordnung:

Inhaltsübersicht

§ 1
Gegenstand und Geltungsbereich

(1) Die Regelungen dieser Verordnung und der dazu erlassenen Ausführungsbestimmungen sollen die sichere Nutzung der in der Bremischen Evangelischen Kirche eingesetzten Informationstechnik gewährleisten und die Einhaltung der technischen und organisatorischen Anforderungen an den Datenschutz sicherstellen.

(2) [1]Die IT-Sicherheitsverordnung sowie die dazu erlassenen Ausführungsbestimmungen gelten für die Gemeinden und gesamtkirchlichen Einrichtungen der Bremischen Evangelischen Kirche. [2]Die Vorschriften sind verbindlich für alle dort tätigen haupt- und ehren-

1 jetzt § 54 Absatz 2
2 Nr. **9.100**.
3 jetzt EKD-Datenschutzgesetz (DSG-EKD) vom 15. November 2017 (ABl. EKD 2017 S. 353)
4 Nr. **1.100**.

amtlich Mitarbeitenden und für Dritte, mit denen die Benutzung von Computern und Netzwerken von Gemeinden und gesamtkirchlichen Einrichtungen vereinbart worden ist.

(3) Die rechtlich selbstständigen Werke und Einrichtungen gemäß § 1 Absatz 2 Satz 2 DSG-EKD[1] sind vom Geltungsbereich der Verordnung ausgenommen und stellen die erforderliche IT-Sicherheit in eigener Verantwortung sicher.

§ 2
IT-Sicherheitsziele

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 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 gelöscht, zerstört oder manipuliert werden.
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 der oder dem jeweiligen Verfügungsberechtigen.
5. die Auswahl, Einführung, Gestaltung und Änderung von Verfahren:
   In die Auswahl und Gestaltung von Verfahren zur Verarbeitung personenbezogener Daten ist die oder der Datenschutzbeauftragte der Bremischen Evangelischen Kirche rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.

1 Nr. **9.100** jetzt § 2 Absatz 1 Satz 3 DSG-EKD

§ 3
IT-Sicherheitsstandard

(1) Je nach Schutzbedarf werden Gebäude, Räumlichkeiten, IT-Systeme und sensible Datenbestände durch geeignete Maßnahmen, insbesondere durch ein restriktives Berechtigungskonzept, geschützt.

(2) [1]Der für die Umsetzung der IT-Sicherheitsziele erforderliche grundlegende Sicherheitsstandard orientiert sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz. [2]Konkretisierungen werden vom Kirchenausschuss verbindlich festgelegt.

(3) Soweit im Einzelfall spezielle darüber hinausgehende oder abweichende Schutzbedarfe vorhanden sind, sollen die Verantwortlichen nach § 4 Absatz 1 diese dokumentieren und den erforderlichen Sicherheitsstandard definieren.

§ 4
Verantwortliche

(1) Verantwortlich für die Umsetzung der Bestimmungen sind für den Bereich der Gemeinden der jeweilige Kirchenvorstand sowie für den Bereich der gesamtkirchlichen Einrichtungen die jeweilige Leitung.

(2) Die nach Absatz 1 Verantwortlichen können ihnen durch diese Verordnung zugewiesene Aufgaben an geeignete Personen übertragen.

§ 5
IT-Anwendende

[1]Alle IT-Anwendenden sind für die sachgerechte Nutzung der verwendeten IT-Systeme verantwortlich. [2]Sie beachten die Sicherheitsvorschriften, unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die nach § 4 Absatz 1 Verantwortlichen. [3]IT-Anwendende nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil.

§ 6
Einsatz von Programmen, Sicherheitsmaßnahmen

(1) [1]Für bestimmte Arbeitsbereiche beschließt der Kirchenausschuss über den Einsatz von Systemen und Anwendungen, die einheitlich im Geltungsbereich dieser Verordnung zu verwenden sind. [2]Andere Systeme und Anwendungen dürfen in diesem Arbeitsbereich nicht eingesetzt werden.

(2) Im Übrigen dürfen Programme und dazugehörige Daten nur in die IT-Systeme übernommen werden, wenn dieses von den nach § 4 Absatz 1 Verantwortlichen beschlossen wurde.

(3) [1]Die Verwendung eines Programms darf nur beschlossen werden, wenn das Programm die geltenden Sicherheitsanforderungen erfüllt und datenschutzrechtliche Vorschriften nicht entgegenstehen. [2]Insbesondere können Programme nur eingesetzt werden, wenn eine anerkannte Zertifizierung vorliegt und, sofern erforderlich, datenschutzrechtliche Genehmigungen eingeholt wurden.

(4) Der Kirchenausschuss kann den Einsatz bestimmter Programme untersagen, soweit die IT-Sicherheit durch die Verwendung gefährdet wird.

(5) [1]IT-Sicherheitsmaßnahmen, insbesondere die Entscheidung über den Einsatz von Programmen, sind erst nach erfolgter Beratung durch die Kirchenkanzlei zu treffen. [2]Eine solche Beratung soll die Beachtung von Sicherheitsbestimmungen sicherstellen sowie finanzielle Nachteile und organisatorische Schwierigkeiten vermeiden helfen.

(6) Die Verantwortlichen nach § 4 Absatz 1 legen die Zugriffsberechtigungen für die einzelnen IT-Anwendungen und IT-Systeme fest und bestimmen fachlich qualifizierte Personen, die in dem ihnen zugewiesenen Bereich dafür zuständig sind, dass durch geeignete Maßnahmen der festgelegte Sicherheitsstandard realisiert und aufrecht erhalten wird (Administratoren).

§ 7
Einhaltung der IT-Sicherheitsverordnung

(1) [1]Die Aufsicht über die Einhaltung der Vorschriften zur IT-Sicherheit führt der Kirchenausschuss. [2]Er bedient sich dabei der Kirchenkanzlei.

(2) [1]Die Kirchenkanzlei berät die Verantwortlichen über den Einsatz von Programmen sowie bei Bedarf über Fragen des erforderlichen Sicherheitsstandards nach § 3 Absatz 2 und 3 und über geeignete Maßnahmen zur Beseitigung von Sicherheitsverstößen. [2]Die Kirchenkanzlei ist berechtigt, zur Erstellung einer aktuellen Übersicht zu der im Einsatz befindlichen Informationstechnik und deren Sicherung Erhebungen durchführen.

(3) [1]Der Kirchenkanzlei sind alle zur Durchführung der Aufsicht erforderlichen Informationen zur Verfügung zu stellen und, soweit notwendig, Einsicht in die IT-Systeme zu gewähren. [2]Regelungen zum Mitarbeiterdatenschutz bleiben unberührt.

(4) [1]Bei Verstößen gegen die IT-Sicherheitsverordnung sind vorbehaltlich arbeits- oder dienstrechtlicher und datenschutzrechtlicher Konsequenzen folgende Maßnahmen möglich:

1. Weniger schwerwiegende, insbesondere geringfügige individuelle Verstöße können mündlich beanstandet werden.

2. Bei schwerwiegenden Verstößen sowie bei fortgesetzten oder wiederholten geringfügigen Verstößen kann die Kirchenkanzlei die Verantwortlichen nach § 4 Absatz 1 schriftlich auffordern, den Missstand innerhalb einer angemessenen Frist zu beheben.
3. Wird innerhalb der nach Nummer 2 gesetzten Frist keine Abhilfe geschaffen, erfolgt eine Mitteilung an den Kirchenausschuss, der die unverzügliche Beseitigung des Missstandes anordnen und Maßnahmen nach Nummer 4 für den Fall der Zuwiderhandlung ankündigen kann.
4. Bei fortgesetztem Verstoß trotz Anordnung nach Nummer 3 kann der Kirchenausschuss, sofern die erforderliche IT-Sicherheit anders nicht gewährleistet werden kann, die vorübergehende Sperrung der persönlichen Zugangsberechtigung zur Datenverarbeitungsanlage beschließen oder anordnen, das System außer Betrieb zu nehmen, bis der Nachweis über die Beseitigung des Missstandes erbracht ist.

[2]Über Maßnahmen nach Nummer 2 bis 4 ist die oder der Datenschutzbeauftragte der Bremischen Evangelischen Kirche zu informieren.

§ 8
Ausführungsbestimmungen

[1]Der Kirchenausschuss erlässt Ausführungsbestimmungen zu dieser Verordnung. [2]Die Kirchenkanzlei wird beauftragt, bei Bedarf Merkblätter zu deren Konkretisierung herauszugeben.

§ 9
Inkrafttreten

Diese Verordnung tritt am 1. April 2011 in Kraft.