**6. Tagung der III. Landessynode**
**der Evangelischen Kirche in Mitteldeutschland**
**vom 22. bis 25. November 2023 in Erfurt** **Drucksachen-Nr. 8.8/2**

# Digitalisierungsgesetz - Begründung

## Allgemeines

Digitales Arbeiten ist eine Selbstverständlichkeit und gewinnt weiter rasant an Bedeutung. Den wachsenden Möglichkeiten und Chancen digitaler Arbeitsformen stehen dabei auch steigende Anforderungen und Gefahren gegenüber. Dies lässt sich im staatlichen und gesellschaftlichen Bereich wie auch im kirchlichen Kontext feststellen – seien es teilweise auch unvermutete Fortschritte im Zuge der Corona-Pandemie oder die allwöchentlichen Nachrichten über Sicherheitsvorfälle. Mit dem vorgeschlagenen Kirchengesetz werden grundlegende Regelungen zu den Zuständigkeiten, der Organisation der Weiterentwicklung und des Austauschs über digitale Arbeits- und Kommunikationsmittel aufgestellt. Aufgrund der zunehmenden Bedeutung digitaler Arbeitsformen und angesichts steigender Anforderungen an einen rechtskonformen, dem Stand der Technik entsprechenden Betrieb (Finanzierung, Verantwortung, Verwaltung, Datenschutz, IT-Sicherheit, Lizensierung) soll so ein planmäßiger und effizienter Umgang mit dem Thema Digitalisierung ermöglicht werden.

Das vorgeschlagene Kirchengesetz enthält deshalb neben grundsätzlichen Regelungen zu Ziel und Aufgabe der Digitalisierung einen Abschnitt zur Organisation der Weiterentwicklung digitaler Arbeitsformen, einen Abschnitt zu der Verteilung der Zuständigkeiten hinsichtlich der Bereitstellung und Nutzung digitaler Arbeitsmittel und einen Abschnitt zur IT-Sicherheit. Vergleichbare Regelungen sind im überwiegenden Teil anderer Landeskirchen in Anwendung. Eckpunkte in diesen anderen Landeskirchen sind dabei, dass auf landeskirchlicher Ebene ein dauerhafter Prozess zur planmäßigen Weiterentwicklung digitaler Arbeitsformen organisiert wird, es landeskirchenweite Standardanwendungen und Vereinheitlichungen gibt und Pflichten sowie Verantwortungsbereiche formuliert werden.

## Im Einzelnen:

In **§ 1** wird der Anwendungs- und Geltungsbereich festgelegt. Neben dem verfasst-kirchlichen Bereich besteht für zugeordnete rechtlich selbständige Werke und Einrichtung die Möglichkeit, sich dem Anwendungsbereich des Gesetzes zu unterstellen. Inhaltlich ist festzuhalten, dass Digitalisierung als Querschnittsthema auch viele weitere zu beachtende Regelungsbereiche berührt: die Rechte der Mitarbeitervertretung nach dem Mitarbeitervertretungsgesetz, der Schutz personenbezogener Daten nach dem Datenschutzgesetz der EKD, haushalterische Vorgaben aus dem HKRG oder auch die unabhängige Stellung des Rechnungsprüfungsamtes nach Art. 88 Abs. 2 Kirchenverfassung. Diese gehen dem vorliegenden Kirchengesetz wegen ihrer Spezialität oder ihres höheren Ranges vor.

**Abschnitt 1** enthält grundlegende Festlegungen. **§ 2** stellt die Zweckgebundenheit des Einsatzes digitaler Arbeitsmittel fest und seinen Bezug zum Auftrag der Kirche dar, womit gleichzeitig die ethisch-theologische Perspektive auf Sinn und Grenzen der Digitalisierung einbezogen ist. Der Einsatz von Informations- und Kommunikationstechnik erfasst sowohl das unmittelbar verkündigende Handeln, wie er auch organisierende und verwaltenden Funktionen hat. Die Maßstäbe gelingender Digitalisierung sind in Abs. 3 benannt. Dabei wurde auf Oberbegriffe zurückgegriffen. Der Versuch einer auf Vollständigkeit bedachten Auflistung der im Rahmen der Digitalisierung zu beachtenden Perspektiven wurde nicht unternommen. Abs. 4 hält sodann fest, dass bei der Berücksichtigung der Nutzerperspektiven nicht nur die beruflichen Nutzer zu beachten sind, sondern auch die ehrenamtlichen Nutzer.

Grundsätzlich ist die jeweilige kirchliche Körperschaft für den Einsatz und die Anschaffung digitaler Arbeitsmittel und -verfahren zuständig (**§ 3**). Dabei sind im Interesse eines effizienten Entscheidungsweges und Einsatzes die in § 3 Abs. 2 aufgegebenen Maßgaben zu berücksichtigen, insbesondere auch um örtliche oder kirchliche „Insel-Lösungen", die anschließend einen erhöhten Verwaltungsaufwand nach sich ziehen, zu vermeiden. Aus der Perspektive der IT-Sicherheit kann das Landeskirchenamt Mindestanforderungen festlegen, und damit u. a. veraltete Systeme ausschließen oder in ihrem Einsatz beschränken, oder auch den Einsatz von Systemen und Programmen, die mit erheblichen Sicherheitsrisiken verbunden sind, untersagen. Damit wird auf Kategorien des Datenschutzrechts (Vgl. §§ 27, 32 DSG.EKD) und der IT-Sicherheit nach der IT-Sicherheitsverordnung der EKD Bezug genommen, die sich beide wiederum an den allgemeinen Standards im Bereich der IT-Sicherheit orientieren (müssen).

In grundlegenden Bereichen wird durch **§ 4** Abs. 1 der Einsatz einheitlicher Lösungen vorgegeben. Einheitliche Lösungen sind notwendig, da sich teilweise nur so überhaupt eine digitale Bearbeitung ermöglichen oder effizient gestalten lässt. In so identifizierten Bereichen sind Abweichungen begründungs- und genehmigungspflichtig. Die in Abs. 1 aufgezählten Sachbereiche sind teilweise bereits vereinheitlicht (z. B. Meldewesen, Finanzwesen, Personalwesen und Liegenschaftswesen). In anderen Bereichen (IT-Sicherheit, Kommunikation per Mail/Intranet) haben gerade die vergangenen Jahre deren Notwendigkeit gezeigt, indem nur durch gemeinsame Standards ein effizientes, sicheres und von den Dienststellen unterstütztes digitales Arbeiten möglich ist. Indem hierin ein Anschluss- und Benutzungszwang (mit Befreiungsmöglichkeit im Einzelfall) besteht, sind auch steuerrechtliche Fragen geklärt. Durch einheitliche Vorgaben geht ohne Frage Vielfalt verloren. Gleichzeitig sind die Anforderungen an einen rechtskonformen Betrieb in den vergangenen Jahren stark gewachsen und gewinnen durch die zunehmende Vernetzung weiter an Bedeutung – etwa Datenschutzfolgeabschätzungen, Berechtigungskonzepte und Lizenzfragen.

Weitere Bereiche für einheitliche Dienste und Programme können sich ergeben und dann im Verfahren nach Abs. 2 und 3 eingeführt werden. Dabei sind insbesondere im Sinne eines „Investitionsschutzes" Übergangszeiträume für bestehende abweichende Lösungen zu berücksichtigen. Kirchenkreise und der nach § 5 zu bildende Beirat sind zuvor anzuhören, wie auch die betroffenen Anwendergruppen beteiligt werden sollen, soweit sich hierfür ein sinnvoller Gesprächskanal ergibt. Abs. 4 regelt sodann die Kostentragung nach dem Finanzgesetz.

Als zentrales Beratungsgremium zur Weiterentwicklung und Zusammenarbeit auf dem Gebiet der Digitalisierung wird ein Beirat nach **§ 5** eingerichtet. Dieser trifft keine Entscheidungen, sondern bereitet Entscheidungen der jeweils zuständigen Leitungsorgane vor und unterstützt die Leitungsorgane in Fragen der Digitalstrategie und der eher technisch ausgerichteten IT-Strategie. Ziel ist eine planmäßige (Weiter-)Entwicklung digitaler Verfahren. Gleichzeitig kommt ihm eine allgemeine Beratungszuständigkeit und Vernetzungsaufgabe zu. Die Zusammensetzung durch den Landeskirchenrat erfolgt deshalb ebenenübergreifend. Die konkrete Festlegung zur Zusammensetzung ist nicht Teil des Gesetzes, sondern obliegt dem Landeskirchenrat.

In den Folgeregelungen (**§§ 6, 7**) sind die grundlegenden Zuständigkeiten des Landeskirchenamtes und der Kirchenkreise im Bereich der Digitalisierung zusammengefasst. Das Landeskirchenamt ist für die zentrale Bereitstellung der einheitlichen Programme, Dienste und Anwendungen verantwortlich und übernimmt koordinierende Aufgaben. Die Kirchenkreise sind sodann für die Unterstützung der Kirchengemeinden und Mitarbeitenden in ihrem Bereich zuständig. Dabei können sie ebenfalls verbindliche Beschaffungswege für Systeme und Geräte vorgeben, um so die Ausstattung zu vereinheitlichen und Unterstützung zu ermöglichen.

**Abschnitt 2** regelt den Einsatz und die rechtlichen Rahmenbedingungen digitaler Kommunikationsmittel durch die Mitarbeitenden.

**§ 8** regelt die allgemeinen Grundsätze zur Nutzung digitaler Kommunikationsmittel durch Beschäftigte, ein dienstlicher Internetzugang ist grundsätzlich nur dienstlich zu nutzen, eine private Nutzung bedarf der gesonderten

Vereinbarung[1]. Vergleichbares gilt für E-Mail-Konten: Sie sind für die dienstliche Kommunikation einzusetzen. Private Accounts, seien es Accounts bei sog. Freemailern oder auch sonst von den Beschäftigten in eigener Verantwortung betriebene Accounts bei Dritten, sind aufgrund der datenschutzrechtlichen Probleme, der häufig fehlenden Lizensierung für berufliche Zwecke und dem geringen Sicherheitsniveau nicht zulässig. Standardmäßig ist dafür die einheitliche E-Mail-Lösung nach § 4 des Gesetzes einzusetzen. Weitere dienstliche Accounts – etwa die in Verantwortung der Kirchengemeinde bei Dritten angeschafft werden – sind den Beschäftigten dadurch nicht verboten. Indem die Sicherheitsmaßnahmen dort nur eingeschränkt überprüfbar sind, werden sie aber nicht in gleichem Maße die Zusammenarbeit ermöglichen, wie die einheitliche Lösung nach § 4. Die Zugangsberechtigungen werden grundlegend im Landeskirchenamt verwaltet, sodann aber von den Kirchenkreisen (d. h. den Kreiskirchenämtern) verteilt und betreut.

Das Thema dienstliche Kommunikationstechnik wird in **§ 9** geregelt. Der Grundsatz ist in Abs. 1 normiert, nämlich dass für die Verarbeitung dienstlicher Daten dienstliche Technik eingesetzt wird. Verantwortlich für einen regelkonformen Einsatz ist die jeweilige kirchliche Körperschaft (vgl. § 3 Abs. 1), was sich regelmäßig nur durch die Nutzung dienstlicher Kommunikationstechnik sicherstellen lässt. Die Bereitstellung dienstlicher Geräte ist Sache der Dienststelle. Der in Teilbereichen übliche Einsatz privater IT für dienstliche Zwecke ist künftig nur in Randbereichen und bei hinreichender Berücksichtigung von IT-Sicherheit und Datenschutz zulässig. Ein Anspruch des Beschäftigten auf Nutzung seiner privaten IT besteht nicht, genauso wie er auch nicht zur dienstlichen Nutzung seiner Privatgeräte verpflichtet ist oder sie von ihm erwartet werden kann. Vielmehr bedarf ein dienstlicher Einsatz privater Geräte des Einverständnisses beider Seite und des Abschlusses einer Vereinbarung nach Abs. 3, die unter Berücksichtigung des Schutzbedarfs nach der IT-Sicherheitsverordnung Mindestanforderungen genügen muss. Weitere Rahmenbedingungen ergeben sich aus Abs. 4 und 5.

Neben der Ausstattung von Beschäftigten ist auch bei Ehrenamtlichen eine auf ihre Situation angepasste Ausstattung mit Kommunikationsverfahren und ggf. sogar Technik notwendig. Die bei Beschäftigten unbedingte Pflicht wird nach **§ 10** Abs. 1 zur Soll-Vorschrift. Wenn sich die ehrenamtliche Mitarbeit jedoch auf besonders vertrauliche oder schützenswerte Datenbestände bezieht, sind die Ehrenamtlichen mit der entsprechenden Kommunikationssoftware und den notwendigen Zugängen auszustatten. Regelmäßiges Beispiel sind Seelsorgedaten und wegen der nicht nur gelegentlichen Personalverantwortung die Mitgliedschaft in den genannten Leitungsgremien oder besondere Funktionen. Eine Ausstattung mit dienstlichen IT-Geräten ist regelmäßig nicht erforderlich, sondern der Zugriff bspw. über eine Weboberfläche reicht aus. Bei Zugriff auf besonders sensible Daten können hier aber Grenzen entstehen, die dann doch eine dienstliche Ausstattung mit Technik erforderlich machen.

**Abschnitt 3** befasst sich mit dem immer wichtiger werdenden Feld der IT-Sicherheit. Der Schutzbedarf digitaler Daten erfordert angemessene technische und organisatorische Maßnahmen der IT-Sicherheit und die Nachweisführung über die ergriffenen Maßnahmen (Vgl. § 27 DSG.EKD). Dies ist Aufgabe und Verantwortung jeder kirchlichen Stelle, was in **§ 11** Abs. 1 S. 1 klargestellt wird. Die jeweilige kirchliche Stelle ist allgemein bereits aus dem Datenschutzgesetz zur Nachweisführung im Rahmen eines IT-Sicherheitskonzeptes verpflichtet. Der dabei zu ergreifende Aufwand bemisst sich nach der Größe der jeweiligen Stelle und dem Schutzbedarf der verarbeiteten Daten. Das Landeskirchenamt wird nach § 11 zur Bereitstellung von Mustern verpflichtet, wodurch sich der Aufwand gerade auch für Kirchengemeinden begrenzen lässt. Kirchenkreise und die Landeskirche haben sicherzu-

---

[1] Hintergrund ist, dass mit der erlaubten Privatnutzung Pflichten nach dem Telekommunikationsgesetz einhergehen können. Die Dienststelle wird bei erlaubter Privatnutzung gegenüber dem Beschäftigten rechtlich zum Telekommunikationsanbieter und muss im TKG geregelte Anforderungen erfüllen. Gleichwohl kann die Dienststelle eine Privatnutzung in begrenztem Umfang zulassen, wiewohl der Bedarf aufgrund der allseitigen Verfügbarkeit auch privater Internetzugänge mittlerweile stark zurückgegangen ist.

stellen, dass die Funktion eines IT-Sicherheitsbeauftragten wahrgenommen wird. Es liegt nahe, dass die Kirchenkreise diese Aufgabe bspw. beim gemeinsam betriebenen Kreiskirchenamt ansiedeln. Es besteht aber auch die Möglichkeit einer externen Beauftragung Dritter.

Die Zuständigkeitsverteilung zwischen Landeskirche und Mittlerer Ebene ist in den **§§ 12, 13** geregelt. Insoweit werden die anderen kirchlichen Stellen von Aufgaben der IT-Sicherheit nach § 11 Abs. 1 S. 1 entlastet. Indem Sicherheitsvorfälle gravierende Auswirkungen auf alle Beteiligten haben können, wird in **§ 14** die Anwendbarkeit des Verwaltungs- und Aufsichtsgesetzes konkret festgehalten.

**§ 15** im vierten Abschnitt regelt Überganszeiträume für bestehende Geräte und Systeme und die Pflichten der Kirchenkreise.