

Nomok@non

WEB-JOURNAL

FÜR RECHT

UND RELIGION

FACHARTIKEL

DIGITALISIERUNG IM KIRCHLICHEN VERWALTUNGSRECHT

Staatliche Regelungsmodelle als Vergleichsmaßstab

MICHAEL-ANDREAS NOBEL

ISSN 2749-2826, DOI [10.5282/nomokanon/361](https://doi.org/10.5282/nomokanon/361)

veröffentlicht am 03.08.2026

DIGITALISIERUNG IM KIRCHLICHEN VERWALTUNGSRECHT

Staatliche Regelungsmodelle als Vergleichsmaßstab

VON: MICHAEL-ANDREAS NOBEL

Zusammenfassung: Eine Digitalisierung kirchlicher Verwaltung wirft die Frage auf, ob elektronische Kommunikations-, Dokumentations- und Verwaltungsverfahren mit den Anforderungen des kanonischen Rechts vereinbar sind. Maßgeblich sind dabei nicht allein die verwendeten technischen Mittel, sondern die rechtlichen Sicherungsfunktionen von Schriftlichkeit, Unterzeichnung, notarieller Mitwirkung, Mitteilung, Dokumentation und Archivierung. Untersucht werden sowohl Verwaltungsakte im engeren Sinn als auch Akte der Verwaltung. Unter Berücksichtigung des Kirchlichen Datenschutzgesetzes sowie einschlägiger Vorschriften des deutschen Bundesrechts und des bayerischen Landesrechts wird geprüft, ob digitale Verfahren diese Funktionen in gleichwertiger Weise erfüllen können. Entscheidend sind insbesondere die eindeutige Zurechenbarkeit, Authentizität und Integrität elektronischer Dokumente, die Nachweisbarkeit ihrer Mitteilung, ein geregelter Zugriff sowie angemessene technische und organisatorische Schutzmaßnahmen. Digitale Verfahren sind danach nicht grundsätzlich ausgeschlossen, setzen jedoch voraus, dass die vom kirchlichen Recht geforderten Sicherungszwecke funktional gleichwertig gewährleistet werden.

Summary: The digitalization of ecclesiastical administration raises the question whether electronic communication, documentation and administrative procedures are compatible with the requirements of canon law. The issue is not the technology itself, but whether the legal functions traditionally ensured by written form, signatures, notarial participation, notification, documentation and archiving can be preserved in a digital environment. The analysis encompasses both singular administrative acts and acts of administration. With particular reference to the Church Data Protection Act (KDG), as well as relevant provisions of German federal law and Bavarian state law, it examines whether digital procedures can fulfil these legal functions in a functionally equivalent manner. Particular attention is given to the attribution, authenticity and integrity of electronic documents, the proof of lawful notification, controlled access, and appropriate technical and organizational safeguards. It concludes that digital procedures are not excluded in principle, provided that they ensure the legal safeguards required by canon law in a functionally equivalent manner.

1 Einleitung

Die zunehmende Digitalisierung prägt heute nahezu alle Bereiche administrativen Handelns. Die kirchliche Verwaltung bleibt von dieser Entwicklung nicht unberührt. Elektronische Kommunikation, digitale Aktenführung, Online-Zustellung von Dokumenten sowie der Einsatz moderner Informationssysteme gehören mittlerweile zum praktischen Alltag zahlreicher kirchlicher Institutionen. Mit diesen Entwicklungen entstehen zugleich neue rechtliche Fragestellungen, insbesondere hinsichtlich des Datenschutzes, der Dokumentensicherheit und der rechtlichen Verlässlichkeit elektronischer Verfahren.

Zu prüfen ist daher, ob moderne Kommunikations- und Informationstechnologien mit den Anforderungen des kirchlichen Verwaltungsrechts vereinbar sind. Zunächst mag dies als technische Frage erscheinen. Tatsächlich betrifft sie jedoch vor allem die rechtlichen Sicherungsfunktionen kirchlicher Verwaltung.

Betroffen sind sowohl Akte der Verwaltung, etwa notarielle Dokumentationen, Protokolle, Registerführung und Archivierung, als auch Verwaltungsakte im engeren Sinne, insbesondere Dekrete, Reskripte oder sonstige Verwaltungsentscheidungen. In beiden Bereichen sieht das kanonische Recht bestimmte formale Sicherungen vor, die der Authentizität, Integrität und Beweisbarkeit kirchlicher Verwaltungsvorgänge dienen. Dabei geht es nicht um Formvorschriften als Selbstzweck, sondern um die rechtliche Verlässlichkeit kirchlichen Verwaltungshandelns. In der Diskussion über digitale Verwaltungsverfahren tritt dieser Gesichtspunkt häufig in den Hintergrund.

Die Digitalisierung kirchlicher Verwaltung vollzieht sich nicht losgelöst von staatlichen Rechtsentwicklungen. § 2 Abs. 1 Verwaltungsverfahrensgesetz (VwVfG)¹ bestimmt als Folge des verfassungsmäßig gesicherten Selbstbestimmungsrechts ausdrücklich, dass das Verwaltungsverfahrensgesetz für die Tätigkeit der Kirchen und Religionsgemeinschaften nicht gilt. Kirchliche Verwaltungsakte beruhen daher auf eigenständigen kirchenrechtlichen Kompetenznormen, insbesondere auf der ausführenden Gewalt gemäß c. 35 CIC. Das staatliche Verwaltungsrecht belegt seit Jahren, dass elektronische Verwaltungsverfahren rechtlich beherrschbar sind.² Die dort entwickelten Lösungsansätze bieten daher einen hilfreichen Vergleichsmaßstab, ohne dass dadurch die Eigenständigkeit des kirchlichen Rechts in Frage gestellt würde.

Ein aufschlussreicher Vergleich ergibt sich im Notarrecht. Die Bundesnotarordnung (BNotO)³ beschreibt den Notar als „unabhängige[n] Träger eines öffentlichen Amtes“ und verbindet notarielle Tätigkeit mit Beurkundung, Beglaubigung, Verschwiegenheit, Aktenführung und öffentlicher Verlässlichkeit.⁴ Gerade deshalb eignet sich das notarielle Recht als staatlicher Vergleichspunkt für jene kirchlichen Funktionen, die durch Kanzler, Notare, Register und Archive wahrgenommen werden. Im staatlichen Recht wird Digitalisierung nicht als Auflösung rechtlicher Form verstanden. Elektronische Signaturen, elektronische Aktenführung, elektronische Archive und gesicherte Kommunikationswege treten nicht an die Stelle rechtlicher Sicherungen. Vielmehr werden sie selbst in rechtlich kontrollierte Organisationsstrukturen eingebunden. Der technische Wandel führt daher nicht notwendig zu einem Verlust rechtlicher Verlässlichkeit. Er verändert vielmehr die Art und Weise, wie diese rechtlich abgesichert wird. Für die kirchliche Verwaltung ist dieser Befund deshalb aufschlussreich, weil hier nicht die technische Form als solche im Vordergrund steht, sondern die zuverlässige Wahrung bestimmter rechtlicher Funktionen.⁵

¹ Siehe Verwaltungsverfahrensgesetz (VwVfG) in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. 2003 I S. 102); zuletzt geändert durch: Artikel 2 des Gesetzes vom 15. Juli 2024 (BGBl. 2024 I Nr. 236).

² Vgl. § 3a Abs. 1-3 VwVfG; § 37 Abs. 3 VwVfG.

³ Siehe Bundesnotarordnung (BNotO) n der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-1, veröffentlichten bereinigten Fassung, die zuletzt durch Artikel 2 des Gesetzes vom 10. Dezember 2025 (BGBl. 2025 I Nr. 320) geändert worden ist.

⁴ Vgl. §§ 1, 14 Abs. 1 BNotO.

⁵ Vgl. §§ 33, 35, 78n BNotO; siehe auch Verordnung über die Führung notarieller Akten und Verzeichnisse (NotAktVV) vom 13. Oktober 2020 (BGBl. I S. 2246), die zuletzt durch Artikel 7 des Gesetzes vom 10. Dezember 2025 (BGBl. 2025 I Nr. 320) geändert worden ist; hier §§ 1-6 NotAktVV.

Der Einsatz digitaler Technologien in der kirchlichen Verwaltung ist heute kaum noch die eigentliche Streitfrage. Zu klären bleibt vielmehr, ob digitale Verfahren jene Funktionen zuverlässig erfüllen können, die das kanonische Recht traditionell durch Schriftlichkeit, Mitzeichnung, Dokumentation und Archivierung absichert.

Den kirchlichen Formvorschriften liegen bestimmte Sicherungszwecke zugrunde. Die Schriftlichkeit dient dabei zunächst der dauerhaften Fixierung und Dokumentation eines Verwaltungsvorgangs. Weitere Sicherungsfunktionen, insbesondere hinsichtlich Authentizität, Integrität und Zurechenbarkeit, ergeben sich regelmäßig erst im Zusammenwirken mit Unterschrift, Mitzeichnung, Siegelung, Dokumentation und Archivierung. Erst wenn diese Funktionen bestimmt sind, lässt sich beurteilen, ob moderne Kommunikations- und Informationstechnologien sie in vergleichbarer Weise gewährleisten können. Digitale Verwaltungsverfahren berühren zugleich das Datenschutzrecht. Sowohl das Kirchliche Datenschutzgesetz als auch die staatlichen Datenschutzgesetze knüpfen die digitale Verarbeitung von Informationen an technische und organisatorische Sicherungen, die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit gewährleisten sollen.⁶ Die Untersuchung konzentriert sich daher nicht auf einzelne technische Anwendungen, sondern auf die rechtlichen Schutzgüter, die das kirchliche Verwaltungsrecht sichern will, und unter welchen Voraussetzungen digitale Verfahren diese Funktionen übernehmen können. Da diese Frage in einem genuin kirchenrechtlichen Zusammenhang steht, bildet der Codex den eigentlichen Ausgangspunkt der Untersuchung. Die staatlichen Regelungen werden nicht als tragende Rechtsgrundlage herangezogen, sondern lediglich als Vergleichsmaßstab für die rechtliche Bewältigung digitaler Dokumentation, elektronischer Kommunikation und gesicherter Aktenführung. Im Zentrum der Untersuchung steht daher die kanonistische Frage, welche rechtlichen Funktionen durch die Anforderungen an Schriftlichkeit, Unterzeichnung, notarielle Mitwirkung, Dokumentation und Archivierung geschützt werden. Vor diesem Hintergrund ist zu untersuchen, ob diese Formanforderungen notwendig eine papiergebundene Dokumentation voraussetzen oder ob ihre Sicherungszwecke auch durch digitale Verfahren in funktional gleichwertiger Weise verwirklicht werden können. Daher ist zu prüfen, ob digitale Kommunikations- und Informationstechnologien diese Funktionen in funktional gleichwertiger Weise gewährleisten können.

2 Ausgangspunkt: Formanforderungen im kirchlichen Verwaltungsrecht

Wenn über Digitalisierung in der kirchlichen Verwaltung gesprochen wird, entsteht leicht der Eindruck, es handle sich primär um eine technische Problematik. Tatsächlich liegt der Schwerpunkt jedoch auf der Ebene des Rechts. Im Mittelpunkt steht nicht das verwendete technische Mittel als solches, sondern die Wahrung jener rechtlichen Funktionen, die das kanonische Recht für Verwaltungsakte und sonstige Akte der Verwaltung voraussetzt.

Schon die einschlägigen Vorschriften des Codex binden kirchliches Verwaltungshandeln an Anforderungen der Dokumentation und Sicherung. Ein Verwaltungsakt für Einzelfälle kann nur

⁶ Vgl. Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 3 des Gesetzes vom 12. Mai 2026 (BGBl. 2026 I Nr. 139) geändert worden ist; hier § 64 Abs. 2 Satz 2 Nr. 1 BDSG; § 64 Abs. 3 Satz 1 Nr. 1-14 BDSG.

von demjenigen erlassen werden, der innerhalb der Grenzen seiner Zuständigkeit ausführende Gewalt besitzt.⁷ Der Verwaltungsakt bleibt damit einem konkreten Amtsträger zugeordnet. Hinzu tritt c. 37 CIC, wonach ein Verwaltungsakt des äußeren Bereichs „schriftlich auszufertigen“ ist (*Actus administrativus, qui forum externum respicit, scriptis est consignandus*). Bereits der Wortlaut der Norm legt den Schwerpunkt auf die Schriftlichkeit des Verwaltungsvorgangs, ohne ausdrücklich festzulegen, auf welchem Trägermedium diese Schriftlichkeit zu erfolgen hat. Das Gesetz spricht von der schriftlichen Fixierung des Verwaltungsaktes, nicht jedoch von Papier als zwingendem Träger dieser Schriftlichkeit. Wird ein Verwaltungsakt im Auftragsweg vollzogen, ist der Vollzugsakt schriftlich festzuhalten. Für Dekrete konkretisiert c. 51 CIC diese Vorgabe weiter. Sie sind „schriftlich zu erlassen“ und, soweit sie eine Entscheidung enthalten, wenigstens summarisch zu begründen. Bereits diese wenigen Vorschriften unterstreichen die Bedeutung der Dokumentation für das kirchliche Verwaltungsrecht. Allerdings lässt sich den genannten Vorschriften noch nicht unmittelbar entnehmen, welche Bedeutung dem materiellen Träger der Dokumentation zukommt. Die Normen setzen damit bestimmte Formelemente voraus. Offen bleibt jedoch, ob diese Formelemente ausschließlich durch papiergebundene Dokumente verwirklicht werden können oder ob andere technische Trägerformen in Betracht kommen.

Die Mitteilung des Verwaltungsaktes besitzt zudem eine erhebliche rechtliche Bedeutung. Nach c. 54 CIC entfaltet ein Dekret mit dem Vollzug Rechtswirkung, wenn seine Anwendung einem Vollzieher übertragen ist. Anderenfalls tritt die Rechtswirkung mit der Mitteilung durch die entscheidende Autorität ein. Die rechtliche Relevanz des Verwaltungshandelns erschöpft sich daher nicht im Erlass des Aktes selbst. Problematisch erscheint, ob und in welcher Weise dieser Akt nach außen vermittelt und später nachgewiesen werden kann.

Die kanonischen Vorschriften beschränken sich allerdings nicht auf den Verwaltungsakt selbst. Sie regeln zugleich die institutionellen Rahmenbedingungen, innerhalb derer kirchliche Verwaltung stattfindet. C. 474 CIC bestimmt ausdrücklich, dass entsprechende Akten „vom Ordinarius zu unterzeichnen und vom Kanzler oder einem Notar gegenzuzeichnen sind.“ Der Gesetzgeber knüpft die Wirksamkeit des Aktes damit an dessen rechtliche Zurechenbarkeit und amtliche Authentifizierung. Die Norm schützt zunächst die verlässliche Zuordnung des Verwaltungshandelns zu den zuständigen Amtsträgern; eine ausdrückliche Bindung an die Papierurkunde enthält sie demgegenüber nicht. Die cc. 482-484 CIC konkretisieren die Aufgaben des Kanzlers und der Notare näher. Deren Tätigkeit besteht nicht lediglich in der technischen Erstellung von Dokumenten. Ihnen kommt vielmehr eine besondere Verantwortung für die Ausfertigung, Dokumentation und Verwahrung kirchlicher Akten zu.⁸

Die Archivnormen der cc. 486-491 CIC ergänzen diesen Rahmen. Sie verlangen die geordnete Aufbewahrung kirchlicher Dokumente, die Sicherung des Archivs und die Führung entsprechender Verzeichnisse.⁹ Im Zusammenhang gelesen regeln diese Vorschriften nicht nur die Entstehung eines Verwaltungsaktes. Zu untersuchen bleibt, wie dessen Herkunft, Inhalt und Fortbestand gesichert werden können. Die Formvorschriften des kirchlichen Verwaltungsrechts verfolgen damit erkennbar mehr als bloße Ordnungsgesichtspunkte. Sie sichern die Beweisbarkeit kirchlichen Verwaltungshandelns. Vergleichbare Überlegungen finden sich im staatlichen Verwaltungsrecht dort, wo die Bestimmbarkeit der erlassenden Behörde, die

⁷ Vgl. c. 35 CIC.

⁸ Vgl. c. 482 §1 CIC; c. 484 nn. 1-3 CIC.

⁹ Vgl. c. 486 §1-3 CIC; cc. 487-491 CIC.

Dokumentation behördlicher Entscheidungen oder deren spätere Nachprüfbarkeit abgesichert werden.¹⁰

Ausgangspunkt ist somit die Herkunft eines Verwaltungsaktes. Kirchliches Verwaltungshandeln setzt voraus, dass ein Akt eindeutig demjenigen zugerechnet werden kann, der zu seinem Erlass befugt ist. Erlässt etwa der Diözesanbischof ein Dekret über die Errichtung einer Pfarrei oder die Ernennung eines Pfarrers, muss feststehen, dass die Entscheidung tatsächlich von ihm ausgegangen ist. Dieser Gedanke liegt c. 474 CIC zugrunde. Die gesetzliche Anordnung verlangt für rechtserhebliche Akte der Kurie die Unterschrift des Ordinarius sowie die Mitunterzeichnung durch den Kanzler oder einen Notar. Man könnte daraus folgern, dass der Gesetzgeber eine traditionelle papiergebundene Dokumentationsform voraussetzt. Die Norm selbst trifft jedoch keine ausdrückliche Aussage darüber, ob diese Sicherungen ausschließlich durch körperliche Dokumente verwirklicht werden können.

Durch die schriftliche Fixierung entsteht zunächst die Grundlage für eine dauerhafte Fixierung des Verwaltungsvorgangs. Die rechtliche Absicherung seiner Herkunft und Verlässlichkeit wird jedoch erst durch die Unterzeichnung und Mitzeichnung gewährleistet. Die Mitzeichnung erschöpft sich dabei nicht in einer verwaltungsinternen Ordnungsvorschrift. Die Norm dient damit letztlich der Verlässlichkeit kirchlichen Verwaltungshandelns. Dass diese Problematik keineswegs auf papiergebundene Verfahren beschränkt ist, zeigt ein Blick in das staatliche Notarrecht. Die Tätigkeit des Notars beruht wesentlich darauf, dass Erklärungen und Dokumente einer bestimmten Person in ihrer amtlichen Funktion zuverlässig zugeordnet werden können. Aus diesem Grund führt der Notar ein Amtssiegel und ist zur Beurkundung, Beglaubigung sowie zur Ausstellung beweiskräftiger Bescheinigungen berufen.¹¹

Durch die Digitalisierung entfällt dieses Problem nicht; es stellt sich lediglich unter veränderten technischen Bedingungen. Nach § 33 Abs. 1 Satz 1 BNotO muss der Notar über ein auf Dauer prüfbares qualifiziertes Zertifikat eines qualifizierten Vertrauensdiensteanbieters sowie über die technischen Mittel zur Erstellung und Validierung qualifizierter elektronischer Signaturen verfügen. Das Zertifikat muss ihn zugleich ausdrücklich als Notar ausweisen.¹² Die elektronische Signatur ersetzt damit nicht lediglich die handschriftliche Unterschrift. Sie dient vielmehr dazu, die Verbindung zwischen Dokument, Amt und handelnder Person im elektronischen Umfeld nachvollziehbar zu sichern.

Hieraus ergibt sich freilich keine unmittelbare Übernahme in das kirchliche Verwaltungsrecht. Die notariellen Vorschriften machen jedoch einen allgemeinen Rechtsgedanken greifbar. Die Frage der Authentizität verschwindet durch Digitalisierung nicht. Sie stellt sich lediglich in anderer Form.¹³ Die praktischen Grenzen elektronischer Verwaltung werden hier deutlich. Wird

¹⁰ Vgl. § 37 Abs. 1 und 3 VwVfG.

¹¹ Vgl. §§ 2, 20, 21 BNotO.

¹² Vgl. § 33 Abs. 1 Satz 1 und 3 BNotO.

¹³ Siehe Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 23.07.2014 (Amtsblatt der Europäischen Union, L 257, 73); zuletzt geändert durch: Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (Amtsblatt der Europäischen Union, L 1183, 1). Die sogenannte eIDAS-Verordnung definiert die elektronische Signatur als Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verbunden werden und vom Unterzeichner zum Unterzeichnen verwendet werden (Art. 3 Nr. 10 eIDAS-VO). Für fortgeschrittene elektronische Signaturen verlangt Art. 26 eIDAS-VO insbesondere die eindeutige Zuordnung zum Unterzeichner, dessen

ein Dekret lediglich als gewöhnliche E-Mail versandt, ist zwar ein Text übermittelt. Ob dieser tatsächlich vom zuständigen Amtsträger stammt, bleibt dagegen häufig offen. Die technische Möglichkeit der Übermittlung beantwortet noch nicht die rechtliche Frage nach der Herkunft des Dokuments. Aus diesem Grund beschränkt sich das staatliche Recht nicht darauf, elektronische Signaturen zuzulassen. Es schützt zugleich die Mittel ihrer Verwendung. Die Bundesnotarordnung untersagt dem Notar, die qualifizierte elektronische Signaturerstellungseinheit oder die entsprechende kryptographische Hardwarekomponente einer anderen Person zu überlassen oder Identifikationsdaten preiszugeben. Die technische Absicherung verfolgt damit letztlich einen juristischen Zweck: Die persönliche Zurechenbarkeit amtlichen Handelns soll unter digitalen Bedingungen erhalten bleiben.¹⁴

Zu klären ist, ob der Inhalt eines Verwaltungsaktes unverändert erhalten bleibt. Selbst wenn feststeht, von wem ein Dokument stammt, bleibt offen, ob sein Inhalt später noch mit dem ursprünglich erlassenen Akt übereinstimmt. Gerade bei Verwaltungsakten kann dies erhebliche rechtliche Folgen haben. Würde etwa ein Ernennungsdekret nachträglich abgeändert, ohne dass die Änderung erkennbar dokumentiert wird, ließe sich später kaum noch zuverlässig feststellen, welcher Inhalt tatsächlich Rechtswirkung entfaltet hat.

Mehrere Vorschriften des Codex greifen diese Problematik auf. C. 40 CIC verlangt vom Vollzieher eines Verwaltungsaktes, dass er das Schriftstück erhält und vor seinem Tätigwerden „die Echtheit und Unversehrtheit der Urkunde geprüft hat“ (*integritate et authenticitate litterarum inspectis*). Der Gesetzgeber beschränkt sich damit nicht auf den Sachverhalt der Herkunft eines Dokuments. Ebenso wichtig ist die Gewissheit, dass der Inhalt unverändert geblieben ist. Die Frage der Integrität stellt sich damit nicht erst bei der Archivierung oder späteren Verwendung eines Verwaltungsaktes, sondern bereits im Rahmen seines Vollzugs. Die kanonischen Vorschriften beschreiben insoweit das zu schützende Rechtsgut, nicht jedoch die technischen Mittel seiner Sicherung. Welche Anforderungen daraus für digitale Verfahren folgen, bedarf daher einer eigenständigen Auslegung. In dieselbe Richtung weisen die Archivvorschriften der cc. 486-491 CIC. Sie beschränken sich nicht auf die Forderung, Dokumente aufzubewahren. Verlangt werden vielmehr eine geordnete Verwahrung, kontrollierter Zugang sowie besondere Schutzmaßnahmen für vertrauliche und geheime Unterlagen. Dahinter steht die Vorstellung, dass kirchliche Verwaltungsdokumente nach Jahren noch in einem Zustand vorhanden sein müssen, der eine zuverlässige Feststellung ihres Inhalts und ihres rechtlichen Zusammenhangs erlaubt. Die damit verbundenen Anforderungen stellen sich im digitalen Bereich in besonderer Weise. Elektronische Dokumente können grundsätzlich leichter verändert, kopiert oder in unterschiedlichen Fassungen gespeichert werden als papiergebundene Unterlagen. Eine elektronische Verwaltung ist deshalb nicht notwendig weniger verlässlich. Die Integrität eines Dokuments muss jedoch auf andere Weise gesichert werden.

Das deutsche Notarrecht bietet hierfür einen hilfreichen Vergleich. Nach § 35 Abs. 1 Satz 1 BNotO sind Akten und Verzeichnisse so zu führen, dass ihre Verfügbarkeit, Integrität, Transparenz und Vertraulichkeit gewährleistet bleiben. Die Norm reicht allerdings über das Notarrecht hinaus. Elektronische Aktenführung erschöpft sich nicht in der Speicherung digitaler Dokumente. Sie

Identifizierbarkeit sowie die Erkennbarkeit nachträglicher Veränderungen der signierten Daten. Damit verbindet die Verordnung elektronische Authentizität mit persönlicher Zurechnung und Integritätsschutz.

¹⁴ Vgl. § 33 Abs. 4 BNotO. Art. 46 eIDAS-VO verlangt, dass qualifizierte elektronische Signaturerstellungseinheiten die Signaturstellungsdaten gegen eine Verwendung durch andere verlässlich schützen; vgl. Anhang II Nr. 1 Buchst. d eIDAS-VO.

setzt Strukturen voraus, die Änderungen nachvollziehbar machen, Bearbeitungsvorgänge dokumentieren und unbefugte Eingriffe verhindern.¹⁵ Gerade für kirchliche Verwaltungsdokumente erscheint dieser Gedanke naheliegend. Ein elektronisches Dokument kann seine Funktion nur erfüllen, wenn nicht lediglich seine Herkunft, sondern die Unverändertheit seines Inhalts nachvollziehbar bleibt. Moderne Dokumentenmanagementsysteme versuchen dies etwa durch Versionierung, Protokollierung oder abgestufte Zugriffsrechte zu gewährleisten. Demgegenüber würde eine Ablage in frei bearbeitbaren Dateien, deren Änderungen weder kontrolliert noch dokumentiert werden, den Sicherungszwecken des kirchlichen Verwaltungsrechts kaum gerecht werden.¹⁶

Kirchliche Verwaltungsakte werden nicht nur erlassen und vollzogen. Mitunter werden sie zum Gegenstand späterer Auseinandersetzungen. Dies kann etwa der Fall sein, wenn die Gültigkeit eines Dekrets bestritten wird oder gegen eine Verwaltungsentscheidung hierarchischer Rekurs eingelegt wird. In solchen Situationen genügt es nicht, dass Herkunft und Inhalt eines Dokuments ursprünglich gesichert waren. Ebenso muss feststellbar bleiben, welcher Akt tatsächlich erlassen wurde, welchen Inhalt er hatte und zu welchem Zeitpunkt er rechtlich wirksam geworden ist.

In solchen Fällen entscheidet die Dokumentation darüber, ob ein Verwaltungsvorgang später zuverlässig nachgewiesen werden kann. Das kanonische Recht überlässt die spätere Nachweisbarkeit nicht dem Zufall, sondern bindet sie ausdrücklich an die notarielle Amtsaufgabe. Nach c. 484 CIC haben Notare Akten und Urkunden über Dekrete, Verfügungen und Verpflichtungen anzufertigen, das rechtlich Erhebliche getreu schriftlich festzuhalten sowie Abschriften und Ausfertigungen als mit der Urschrift übereinstimmend zu bestätigen. Die Tätigkeit des Notars erschöpft sich damit nicht in der bloßen Erstellung von Dokumenten. Sie dient zugleich dazu, den maßgeblichen Inhalt eines Verwaltungsvorgangs dauerhaft festzuhalten und für spätere Nachweise verfügbar zu halten.

Die Entwicklung des staatlichen Rechts zeigt, dass die Beweisfunktion nicht an eine bestimmte materielle Form gebunden ist. Die Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO) geht ausdrücklich davon aus, dass elektronische Dokumente und elektronische Signaturen grundsätzlich als Beweismittel geeignet sein können. Nach Art. 25 Abs. 1 eIDAS-VO darf einer elektronischen Signatur die Rechtswirkung und die Zulässigkeit als Beweismittel nicht allein deshalb abgesprochen werden, weil sie elektronisch vorliegt oder nicht die Voraussetzungen einer qualifizierten elektronischen Signatur erfüllt. Für qualifizierte elektronische Signaturen ordnet Art. 25 Abs. 2 eIDAS-VO zudem die gleiche Rechtswirkung wie für eine handschriftliche Unterschrift an. Art. 46 eIDAS-VO beruht auf demselben Grundgedanken. Die Normen ersetzen keine kanonischen Formanforderungen. Sie bringen jedoch einen allgemeinen Rechtsgedanken zum Ausdruck, wonach Herkunft, Inhalt und

¹⁵ Die eIDAS-Verordnung verbindet elektronische Sicherungsmittel nicht nur mit Authentizität, sondern ebenso mit Integrität. Elektronische Siegel dienen nach Art. 3 Nr. 25 eIDAS-VO dazu, den Ursprung und die Unversehrtheit elektronischer Daten sicherzustellen. Für qualifizierte elektronische Siegel gilt zudem die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe (vgl. Art. 35 Abs. 2 eIDAS-VO). Damit wird deutlich, dass digitale Sicherungsmittel nicht nur den Absender kenntlich machen, sondern zugleich den unveränderten Bestand des Dokuments absichern können.

¹⁶ Das notarielle Recht vermeidet gerade eine solche Reduktion digitaler Akten auf bloße Dateien. Elektronische Akten und Verzeichnisse dürfen nach § 35 Abs. 4 BNotO außerhalb der Geschäftsstelle nur im Elektronischen Urkundenarchiv oder im Elektronischen Notariatsaktenspeicher geführt werden. Die technische Umgebung wird damit selbst Teil der rechtlichen Sicherung.

Nachvollziehbarkeit eines Dokuments so gesichert sein müssen, dass seine elektronische Form einer rechtlichen Anerkennung nicht von vornherein entgegensteht.

Ein Beispiel hierfür bietet die Mitteilung von Verwaltungsakten. Für die rechtliche Beurteilung eines Dekrets ist häufig nicht nur sein Inhalt von Bedeutung, sondern auch, ob und wann es dem Adressaten wirksam bekanntgegeben wurde. Nach c. 54 CIC entfaltet ein Dekret, dessen Anwendung einem Vollzieher übertragen wird, seine Rechtswirkung mit dem Vollzug. Anderenfalls tritt die Rechtswirkung mit der Mitteilung durch die entscheidende Autorität ein. Die spätere Nachweisbarkeit der Mitteilung kann daher für die Beurteilung des Verwaltungsvorgangs entscheidend sein. Ähnliche Überlegungen finden sich im staatlichen Verwaltungsrecht. Hier hängt die Wirksamkeit eines Verwaltungsaktes grundsätzlich von seiner Bekanntgabe ab.¹⁷ Das Verwaltungszustellungsgesetz (VwZG)¹⁸ konkretisiert diesen Gedanken für schriftliche und elektronische Dokumente. Nach § 2 Abs. 1 VwZG ist Zustellung die Bekanntgabe eines schriftlichen oder elektronischen Dokuments in der gesetzlich vorgesehenen Form. Gerade im elektronischen Bereich stellt sich dabei die praktische Frage, wie Zugang und Zeitpunkt der Übermittlung später nachgewiesen werden können. Während sich der Zugang eines eingeschriebenen Briefes regelmäßig vergleichsweise leicht dokumentieren lässt, bestehen bei einfachen elektronischen Nachrichten häufig größere Unsicherheiten. Das Gesetz trägt diesem Umstand Rechnung, indem es den Nachweis von Zugang und Zeitpunkt der Zustellung der Behörde zuweist.¹⁹

Trotz ihrer unterschiedlichen Ausgestaltung laufen die genannten Vorschriften letztlich auf dieselben Grundfragen hinaus. Verwaltungsakte müssen ihrem Urheber zugeordnet, in ihrem Inhalt gesichert und nachträglich noch nachweisbar bleiben.²⁰ Ob diese Funktionen durch papiergebundene oder elektronische Verfahren erfüllt werden, ist zunächst nicht die entscheidende Frage. Ausschlaggebend erscheint vielmehr, ob die eingesetzten Verfahren diese Sicherungsfunktionen gewährleisten. Erst auf dieser Grundlage lässt sich beurteilen, in welchem Umfang digitale Kommunikations- und Informationstechnologien mit den Anforderungen des kirchlichen Verwaltungsrechts vereinbar sind. Die bisher dargestellten Vorschriften geben daher keine abschließende Antwort auf die Zulässigkeit digitaler Verfahren. Sie bestimmen jedoch die rechtlichen Maßstäbe, an denen sich eine solche Beurteilung orientieren muss.²¹

¹⁷ Vgl. § 43 Abs. 1 Satz 1 VwVfG.

¹⁸ Siehe Verwaltungszustellungsgesetz (VwZG) vom 12. August 2005 (BGBl. I S. 2354), das zuletzt durch Artikel 3 des Gesetzes vom 15. Juli 2024 (BGBl. 2024 I Nr. 236) geändert worden ist.

¹⁹ § 4 Abs. 2 Satz 3 VwZG. Vergleichbare Sicherungen enthält das notarielle Kommunikationssystem. Der Zugang zum besonderen elektronischen Notarpostfach darf nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln erfolgen (vgl. § 78n Abs. 2 Satz 1 BNotO). Für qualifizierte Dienste der Zustellung elektronischer Einschreiben gelten zudem die Vermutungen des Art. 43 Abs. 2 eIDAS-VO hinsichtlich Integrität der Daten, Identität von Absender und Empfänger sowie Datum und Uhrzeit der Übermittlung. Elektronische Kommunikation wird damit rechtlich an Nachweisbarkeit, Identitätssicherung und Integritätsschutz gebunden.

²⁰ Die Bundesnotarordnung und die eIDAS-Verordnung zeigen übereinstimmend, dass elektronische Signaturen, elektronische Dokumente und gesicherte Kommunikationswege rechtlich nicht wegen ihrer digitalen Form bewertet werden, sondern nach ihrer Fähigkeit, Authentizität, Integrität und Nachweisbarkeit zu gewährleisten.

²¹ Bereits auf der Ebene der Auslegung stellt sich die Frage, ob die genannten Formvorschriften zwingend an papiergebundene Dokumente gebunden sind oder ob sie primär bestimmte rechtliche Funktionen sichern sollen. Nach c. 17 CIC sind kirchliche Gesetze nicht isoliert nach ihrem Wortlaut, sondern nach ihrem Zusammenhang sowie ihrem Ziel und Zweck auszulegen. Die Zulässigkeit digitaler Verfahren ist daher zunächst von der kanonistischen Hermeneutik zu klären, bevor sie technisch umsetzbar wird.

3 Grundsatz der funktionalen Äquivalenz

Die bisher dargestellten Vorschriften folgen einer gemeinsamen Linie. Das kirchliche Verwaltungsrecht verlangt für Verwaltungsakte bestimmte Formelemente, insbesondere Schriftlichkeit, Unterzeichnung und Dokumentation. Die einschlägigen Vorschriften legen jedoch nicht ausdrücklich fest, auf welchem technischen Trägermedium diese Anforderungen verwirklicht werden müssen. Im Vordergrund stehen vielmehr die rechtlichen Funktionen, die durch die jeweiligen Formanforderungen gesichert werden sollen. C. 37 CIC verlangt für Verwaltungsakte des äußeren Bereichs die schriftliche Ausfertigung. Für Dekrete bestimmt c. 51 CIC darüber hinaus, dass sie schriftlich zu erlassen und wenigstens summarisch zu begründen sind. Daraus ergibt sich zunächst lediglich, dass der Gesetzgeber Schriftlichkeit verlangt. Ob diese Schriftlichkeit notwendig eine papiergebundene Urkunde voraussetzt oder auch durch elektronische Dokumente verwirklicht werden kann, lässt sich dem Wortlaut allein nicht eindeutig entnehmen. Der Gesetzgeber spricht von der Schriftlichkeit des Verwaltungsaktes, trifft jedoch keine ausdrückliche Aussage über den materiellen Träger dieser Schriftlichkeit. Bereits deshalb erscheint es nicht selbstverständlich, die Normen ausschließlich auf papiergebundene Dokumente zu beziehen. Eine streng formbezogene Auslegung wäre gleichwohl vertretbar. Sie könnte darauf verweisen, dass der historische Gesetzgeber ausschließlich papiergebundene Verwaltungsverfahren kannte und daher vorausgesetzt hat. Dem lässt sich jedoch entgegenhalten, dass die Normen selbst keine Aussage über bestimmte technische Trägerformen enthalten. Der Wortlaut konzentriert sich vielmehr auf die Schriftlichkeit des Verwaltungsvorgangs. Ob ein elektronisches Dokument die Anforderungen der Schriftlichkeit erfüllen kann, ist vielmehr durch Auslegung der mit der Schriftform verfolgten rechtlichen Zwecke zu beantworten.²² Diese Auslegung entspricht zugleich den allgemeinen Regeln der kanonischen Hermeneutik. Nach c. 17 CIC sind kirchliche Gesetze nach dem Eigenwert ihrer Worte im Text und Zusammenhang auszulegen; bleiben Zweifel bestehen, sind Parallelstellen, Ziel und Zweck des Gesetzes sowie die Umstände seines Erlasses heranzuziehen. Die hier behandelten Vorschriften sprechen zwar von Schriftlichkeit, Unterzeichnung, Dokumentation und Archivierung, äußern sich jedoch nicht ausdrücklich zur Frage des verwendeten technischen Trägermediums. Deshalb erscheint es sachgerecht, die mit diesen Anforderungen verfolgten rechtlichen Sicherungszwecke in die Auslegung einzubeziehen. Gegen diese Auslegung lässt sich allerdings einwenden, dass die einschlägigen Vorschriften des Codex durchgehend von Schriftlichkeit, Unterzeichnung und dokumentierter Aktenführung ausgehen. Ein Vertreter einer streng formbezogenen Auslegung könnte daher argumentieren, dass der universale Gesetzgeber bei Erlass des Codex ausschließlich papiergebundene Verwaltungsverfahren vor Augen hatte. Die in cc. 37 und 51 CIC vorausgesetzte Schriftlichkeit sowie die in c. 474 CIC verlangte Unterzeichnung und Mitunterzeichnung könnten daher als Hinweis darauf verstanden werden, dass kirchliche Verwaltungsakte grundsätzlich in körperlicher Urkundenform zu errichten sind. Solange der kirchliche Gesetzgeber keine ausdrückliche Regelung über elektronische Verwaltungsakte geschaffen hat, ließe sich daraus folgern, dass die Papierurkunde weiterhin den rechtlichen Regelfall bildet. Diese Sichtweise

²² Die cc. 37 und 51 CIC verwenden den Begriff der Schriftlichkeit, ohne den Träger der schriftlichen Erklärung näher zu bestimmen. Die Normstrukturen entstanden zu einem Zeitpunkt, als elektronische Verwaltungsverfahren praktisch keine Rolle spielten. Allein aus diesem historischen Befund lässt sich jedoch noch nicht ableiten, dass der Gesetzgeber ausschließlich papiergebundene Dokumente vor Augen hatte. Entscheidend bleibt daher die Auslegung der mit der Schriftlichkeit verbundenen Sicherungszwecke.

verdient Beachtung, weil das geltende universalkirchliche Recht elektronische Verwaltungsakte tatsächlich nicht ausdrücklich regelt. Sie überzeugt jedoch nicht vollständig. Die genannten Vorschriften bestimmen zwar bestimmte Formanforderungen, äußern sich aber nicht ausdrücklich zur Frage des technischen Trägermediums. Der Wortlaut knüpft an Schriftlichkeit, Unterzeichnung und Dokumentation an, nicht jedoch an Papier als solches. Deshalb erscheint es sachgerechter, die mit diesen Anforderungen verfolgten rechtlichen Sicherungszwecke in den Mittelpunkt der Auslegung zu stellen.

Die hier diskutierte funktionale Betrachtung löst sich nicht vom Gesetzeswortlaut, sondern versucht gerade, dessen Zweck im digitalen Umfeld zu bestimmen. Vergleichbare Überlegungen finden sich in c. 40 CIC. Der Vollzieher eines Verwaltungsaktes darf grundsätzlich erst tätig werden, nachdem er das Schriftstück erhalten und dessen Echtheit sowie Unversehrtheit geprüft hat. Die betreffende Regelung stellt nicht den Papierträger in den Mittelpunkt, sondern die Verlässlichkeit des Verwaltungsvorgangs. Entscheidend ist, dass Herkunft und Inhalt des Aktes feststehen, bevor rechtliche Wirkungen an ihn anknüpfen.

Vergleichbare Überlegungen zeigen sich bei den Vorschriften über Mitteilung und Dokumentation. Nach c. 54 § 2 CIC muss ein Dekret, damit es geltend gemacht werden kann, in einem rechtmäßigen Dokument nach Maßgabe des Rechts mitgeteilt werden. Für Ausnahmefälle regelt c. 55 CIC, dass ein Dekret vor einem Notar oder zwei Zeugen verlesen werden kann, wenn ein schwerwiegender Grund der Aushändigung des schriftlichen Textes entgegensteht. Über die Verlesung ist ein Schriftstück anzufertigen, das von den Anwesenden zu unterschreiben ist. C. 56 CIC behandelt wiederum den Fall, dass ein Adressat ordnungsgemäß geladen wurde, jedoch ohne gerechten Grund nicht erscheint oder die Entgegennahme beziehungsweise Anhörung verweigert. Zusammengefasst folgt aus diesen Vorschriften, dass es dem Gesetzgeber nicht lediglich um die tatsächliche Kenntnisnahme eines Dekrets geht. Die Bekanntgabe muss in einer Form erfolgen, die später noch nachvollzogen werden kann. Die Problematik ist deshalb weniger eindeutig, als es zunächst erscheinen mag. Sowohl eine formbezogene als auch eine stärker zweckorientierte Auslegung lassen sich argumentativ begründen.

Die verschiedenen Regelungen schützen nicht lediglich die äußere Form eines Dokuments. Die Schriftlichkeit gewährleistet zunächst dessen dauerhafte Fixierung und Dokumentation. Weitere Sicherungen ergeben sich aus dem Zusammenwirken der jeweiligen Formvorschriften mit den Anforderungen an Unterzeichnung, Mitwirkung, Mitteilung und Archivierung. Die rechtliche Beurteilung neuer technischer Verfahren kann daher nicht allein von ihrer äußeren Gestalt abhängen. Ob ein Verwaltungsakt auf Papier oder in elektronischer Form vorliegt, beantwortet die kirchenrechtliche Frage daher noch nicht.

Aus dieser Perspektive kommt es für die rechtliche Beurteilung elektronischer Kommunikations- und Dokumentationsformen entscheidend darauf an, ob sie Authentizität, Integrität, rechtmäßige Mitteilung und Beweisbarkeit in vergleichbarer Weise gewährleisten wie die herkömmlichen Formen kirchlicher Verwaltung. Der folgenden Untersuchung liegt die Annahme zugrunde, dass die kanonischen Formvorschriften zwar bestimmte Formelemente voraussetzen, ihr rechtlicher Zweck jedoch nicht primär im Schutz einer bestimmten technischen Trägerform besteht. Maßgeblich erscheinen vielmehr die rechtlichen Sicherungsfunktionen, welche durch Schriftlichkeit, Mitzeichnung, Dokumentation und Archivierung gewährleistet werden sollen. Damit ergibt sich nach der hier vertretenen Auffassung, dass digitale Verfahren grundsätzlich

dort eingesetzt werden können, wo sie diese Funktionen in funktional gleichwertiger Weise erfüllen. Die nachfolgenden Überlegungen dienen der Prüfung dieser These anhand der einschlägigen Vorschriften des kirchlichen Verwaltungsrechts sowie der datenschutz-, archiv- und verwaltungsrechtlichen Vergleichsmaßstäbe.

Dabei ist die funktionale Betrachtung nicht als Übernahme staatlicher Formersatzmodelle zu verstehen. Sie setzt vielmehr bei der kanonistischen Auslegung der einschlägigen Normen an. Die nachfolgend herangezogenen staatlichen Vorschriften finden nicht aufgrund einer Rechtsverweisung des kirchlichen Rechts im Sinne des c. 22 CIC Anwendung. Für die hier behandelten Fragen elektronischer Verwaltungsakte, elektronischer Dokumentation und digitaler Archivierung enthält der Codex keine entsprechende Verweisung. Die staatlichen Regelungen zu elektronischen Dokumenten, Signaturen, Zustellung und Archivierung werden daher ausschließlich als Vergleichsmaßstab herangezogen. Die Entscheidung über die kirchenrechtliche Tragfähigkeit digitaler Verfahren bleibt an Wortlaut, Systematik und Zweck der kanonischen Vorschriften gebunden.

Ein funktionales Verständnis dieser Art prägt das staatliche Recht seit geraumer Zeit.²³ Weder das Verwaltungsrecht noch das Zivilrecht halten grundsätzlich an papiergebundenen Dokumenten fest. Ihr Augenmerk liegt vielmehr daran, unter welchen Voraussetzungen elektronische Formen die Funktionen der herkömmlichen Schriftform übernehmen können. So lässt das Verwaltungsverfahren die Übermittlung elektronischer Dokumente grundsätzlich zu, sofern der Empfänger hierfür einen Zugang eröffnet hat.²⁴ Zugleich bestimmt § 3a Abs. 2 Satz 1 VwVfG, dass eine gesetzlich angeordnete Schriftform durch die elektronische Form ersetzt werden kann, soweit keine abweichende Regelung besteht. Vergleichbare Überlegungen liegen den Vorschriften des Bürgerlichen Gesetzbuchs zugrunde.²⁵ Nach § 126 Abs. 3 Bürgerliches Gesetzbuch (BGB) kann die schriftliche Form grundsätzlich durch die elektronische Form ersetzt werden. § 126a Abs. 1 BGB verlangt hierfür, dass der Aussteller seinen Namen hinzufügt und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versieht. Auf europäischer Ebene wird diese Entwicklung vor allem durch die eIDAS-Verordnung geprägt. Sie regelt unter anderem elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente sowie Dienste für die Zustellung elektronischer Einschreiben.²⁶ Art. 46 eIDAS-VO bringt diesen Ansatz besonders klar zum Ausdruck. Danach darf einem elektronischen Dokument die Rechtswirkung oder die Eignung als Beweismittel nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt. Für elektronische Signaturen verfolgt Art. 25 eIDAS-VO denselben Ansatz. Bereits Abs. 1 untersagt es, einer elektronischen Signatur allein wegen ihrer elektronischen Form die Rechtswirkung oder die Zulässigkeit als Beweismittel abzusprechen. Für qualifizierte elektronische Signaturen ordnet Art. 25 Abs. 2 eIDAS-VO darüber hinaus die gleiche Rechtswirkung wie für eine handschriftliche Unterschrift an. Hieraus lässt sich jedoch nicht ableiten, dass sich diese Regelungen ohne Weiteres auf das kirchliche Verwaltungsrecht

23 Der Rückgriff auf staatliche Regelungen erfolgt dabei nicht als Rechtsquelle des kirchlichen Verwaltungsrechts. Vielmehr dienen diese Vorschriften als Vergleichsmaßstab zur Verdeutlichung rechtlicher Funktionen, die den kanonischen Formanforderungen zugrunde liegen. Die Beurteilung kirchlicher Verwaltungsakte bleibt ausschließlich an den Maßstäben des kirchlichen Rechts orientiert.

24 Vgl. § 3a Abs. 1 VwVfG.

25 Siehe Bürgerliches Gesetzbuch (BGB) in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 12. Mai 2026 (BGBl. 2026 I Nr. 143) geändert worden ist.

26 Vgl. Art. 1 Buchst. c eIDAS-VO.

übertragen ließen. Sie machen jedoch deutlich, auf welcher rechtlichen Überlegung die Anerkennung elektronischer Verfahren beruht. Diese Regelungen knüpfen die rechtliche Bewertung nicht an das Papier als solches. Vielmehr ist festzustellen, ob die Funktionen der jeweiligen Formanforderung weiterhin zuverlässig erfüllt werden.²⁷

Dieselbe Entwicklung lässt sich im Beweisrecht beobachten. Nach § 371a Abs. 1 Zivilprozessordnung (ZPO) sind auf private elektronische Dokumente mit qualifizierter elektronischer Signatur die betreffenden Regelungen über die Beweiskraft privater Urkunden entsprechend anzuwenden.²⁸ Für öffentliche elektronische Dokumente sieht § 371a Abs. 3 ZPO eine entsprechende Anwendung der Vorschriften über öffentliche Urkunden vor, wenn das Dokument in der vorgeschriebenen Form von einer Behörde oder einer mit öffentlichem Glauben versehenen Person erstellt wurde. Das Prozessrecht macht die Beweiswirkung ebenfalls nicht von einem papiergebundenen Urkundenträger abhängig. Herkunft, Echtheit und rechtliche Verlässlichkeit des Dokuments müssen hinreichend abgesichert sein.²⁹ Für das kirchliche Verwaltungsrecht lässt sich daraus kein unmittelbarer Normtransfer ableiten. Die staatlichen Regelungen machen deutlich, dass die rechtliche Bewertung nicht von einer bestimmten technischen Form abhängt. Verlangt der Codex Schriftlichkeit, notarielle Mitzeichnung, Dokumentation oder Archivierung, folgt daraus nicht zwangsläufig die Bindung an eine bestimmte technische Form. Maßgeblich bleibt vielmehr, ob die Funktionen der jeweiligen Vorschrift gewahrt werden. Beispielhaft kann an ein bischöfliches Dekret gedacht werden, das innerhalb eines gesicherten elektronischen Verwaltungssystems erstellt wird. Der Ordinarius kann weiterhin eindeutig identifizierbar bleiben. Ebenso lässt sich die notarielle Mitzeichnung dokumentieren; Veränderungen am Dokument können nachvollziehbar gemacht und die Mitteilung an den Adressaten nachgewiesen werden. Unter solchen Voraussetzungen können Authentizität, Integrität und Beweisbarkeit grundsätzlich ebenso gewährleistet sein wie bei einem papiergebundenen Dokument.

Damit ist jedoch nicht gesagt, dass jede Form elektronischer Kommunikation den rechtlichen Anforderungen genügt. Fehlen die erforderlichen Sicherungen, kann die elektronische Form die rechtlichen Anforderungen nicht erfüllen. Dies gilt insbesondere für Kommunikationswege, bei denen weder die Herkunft eines Dokuments noch dessen Unversehrtheit oder der Zugang beim Empfänger zuverlässig nachgewiesen werden können. Der Mitteilung eines Verwaltungsaktes kommt im kirchlichen Verwaltungsrecht besondere Bedeutung zu. Nach c. 54 CIC tritt die

27 Für den notariellen Bereich wird dieser funktionale Ersatzgedanke besonders deutlich. § 64c Satz 1 BNotO bestimmt, dass eine nach der Bundesnotarordnung oder einer auf ihrer Grundlage erlassenen Rechtsverordnung vorgeschriebene Schriftform auch über das besondere elektronische Notarpostfach ersetzt werden kann, wenn Erklärender und Empfänger über ein solches verfügen. Ist die Erklärung von einer natürlichen Person abzugeben, muss das Dokument entweder mit einer qualifizierten elektronischen Signatur versehen oder von ihr signiert und selbst versendet werden (siehe § 64c Satz 2 BNotO). Die Norm zeigt, dass der elektronische Ersatz der Schriftform nicht durch bloße elektronische Übermittlung erreicht wird. Er setzt vielmehr eine Verbindung von sicherem Kommunikationsweg, persönlicher Zurechnung und dokumentierter Verantwortlichkeit voraus.

28 Siehe Zivilprozessordnung (ZPO) in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 3 des Gesetzes vom 20. Mai 2026 (BGBl. 2026 I Nr. 152) geändert worden ist; hier: § 371a Abs. 1 ZPO.

29 Die Bundesnotarordnung knüpft daran berufs- und organisationsrechtlich an. Nach § 33 Abs. 1 Satz 1 BNotO muss der Notar „über ein auf Dauer prüfbares qualifiziertes Zertifikat eines qualifizierten Vertrauensdiensteanbieters und über die technischen Mittel für die Erstellung und Validierung qualifizierter elektronischer Signaturen verfügen“. Dieses Zertifikat muss zudem mit einem Attribut versehen sein, das den Inhaber als Notar ausweist und Angaben zu Amtssitz, Land und Notarkammer enthält (vgl. § 33 Abs. 1 Satz 3 BNotO). Die elektronische Signatur wird dadurch nicht nur technisch, sondern zugleich amtlich und persönlich verankert. Die elektronische Form kann die Papierform nur dort funktional ersetzen, wo die rechtliche Zurechnung des Dokuments zur verantwortlichen Amtsperson gesichert bleibt.

Rechtswirkung eines Dekretes entweder mit dem Vollzug durch den Vollzieher oder mit der Mitteilung durch die entscheidende Autorität ein. Die bloße Absendung eines Dokuments reicht daher noch nicht aus. Ebenso muss nachvollziehbar bleiben, ob und wann die Mitteilung tatsächlich erfolgt ist. Vergleichbare Anforderungen finden sich im staatlichen Verwaltungsrecht. Dort knüpft die Wirksamkeit eines Verwaltungsaktes ebenfalls an seiner Bekanntgabe an. Elektronische Kommunikationsformen kommen deshalb nur dann in Betracht, wenn Zugang, Zeitpunkt der Übermittlung und die Identität der Beteiligten in rechtlich verlässlicher Weise dokumentiert werden können.³⁰

Aus dem Grundsatz funktionaler Äquivalenz ergibt sich weder ein generelles Verbot digitaler Verfahren noch eine vorbehaltlose Anerkennung jeder Form elektronischer Kommunikation.³¹ Entscheidend bleibt vielmehr, welche Funktion die jeweilige Norm schützen soll. Elektronische Kommunikations- und Dokumentationsformen können dort eingesetzt werden, wo sie die vom kirchlichen Recht geforderten Sicherungszwecke tatsächlich erfüllen. Ob ein Verfahren digital oder papiergebunden ist, beantwortet die rechtliche Frage für sich genommen noch nicht.

4 Zentrale juristische Problemfelder der Digitalisierung im kirchlichen Verwaltungsrecht

Nach Klärung der Grundsatzfrage richtet sich der Blick nun auf die konkreten rechtlichen Schwierigkeiten digitaler Verwaltungsverfahren. Der verstärkte Einsatz digitaler Verfahren wirft Fragen auf, die in der traditionellen Verwaltungsorganisation kaum eine Rolle spielten. Dabei geht es weniger um die technische Funktionsweise elektronischer Systeme als um die Klärung, ob die rechtlichen Anforderungen kirchlicher Verwaltungsnormen unter digitalen Bedingungen zuverlässig erfüllt werden können.

Verwaltungsakte, notarielle Mitwirkung und Archivführung sind dabei als zusammenhängender Regelungskomplex zu betrachten. Gleichwohl verfolgen sie nicht in jeder Hinsicht identische Zwecke. Die Gewichtung einzelner Schutzinteressen kann je nach Regelungszusammenhang unterschiedlich ausfallen. Sie verfolgen jedoch gemeinsame Sicherungszwecke. Sie sichern die Nachvollziehbarkeit kirchlicher Verwaltungsakte unter digitalen Bedingungen. Diese Anforderungen verändern sich durch die Digitalisierung nicht. Sie stellen sich jedoch unter veränderten tatsächlichen Rahmenbedingungen.³² Digitale Verwaltungsvorgänge gehen regelmäßig mit der Verarbeitung personenbezogener Daten einher. Kirchliche Verwaltung bewegt sich daher nicht nur im Anwendungsbereich des Verwaltungsrechts, sondern zugleich

³⁰ Nach § 5 Abs. 5 Satz 1 VwZG kann ein elektronisches Dokument elektronisch zugestellt werden, soweit der Empfänger hierfür einen Zugang eröffnet hat. Dienste für die Zustellung elektronischer Einschreiben erbringen nach Art. 3 Nr. 36 eIDAS-VO den Nachweis der Absendung und des Empfangs und schützen die übermittelten Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung. Für qualifizierte Dienste gilt zudem die Vermutung der Unversehrtheit der Daten, der Absendung durch den identifizierten Absender, des Empfangs durch den identifizierten Empfänger sowie der Richtigkeit von Datum und Uhrzeit der Absendung und des Empfangs (vgl. Art. 43 Abs. 2 eIDAS-VO).

³¹ Soweit der Codex digitale Verwaltungsverfahren nicht ausdrücklich regelt, bedeutet dies nicht notwendig eine bewusste Ablehnung solcher Verfahren. Die kanonische Rechtsordnung kennt mit c. 19 CIC vielmehr einen Auslegungs- und Ergänzungsmechanismus für Fälle, die vom Gesetz nicht ausdrücklich geregelt werden. Die nachfolgende Untersuchung beansprucht nicht, eine Gesetzeslücke durch Analogie zu schließen, macht jedoch deutlich, dass das Fehlen ausdrücklicher Regelungen für digitale Verfahren einer funktionalen Auslegung bestehender Normen nicht entgegensteht.

³² Vgl. cc. 474 und 486 §1 CIC.

innerhalb der Vorgaben des Gesetzes über den Kirchlichen Datenschutz.³³ Bereits § 1 Gesetz über den kirchlichen Datenschutz (KDG) bestimmt den Schutz personenbezogener Daten als Ziel kirchlicher Datenverarbeitung. Nach §§ 2 und 3 KDG erfasst das Gesetz kirchliche Stellen sowie die automatisierte oder sonst strukturierte Verarbeitung personenbezogener Daten. Fragen der digitalen Verwaltungsführung berühren deshalb nicht allein die Organisation kirchlichen Verwaltungshandelns, sondern zugleich die Anforderungen des kirchlichen Datenschutzrechts.

Zunächst geht es um die Zurechenbarkeit kirchlicher Verwaltungsakte. Das kirchliche Verwaltungsrecht setzt voraus, dass ein Verwaltungsakt eindeutig seinem Urheber zugeordnet werden kann und seine Herkunft nachvollziehbar bleibt. Im traditionellen Verwaltungshandeln wird dies vor allem durch Schriftlichkeit, Unterschrift sowie die Mitwirkung des Kanzlers oder eines Notars abgesichert. Unter digitalen Bedingungen stellt sich dieselbe Anforderung erneut, allerdings in veränderter Form. Die bloße technische Möglichkeit elektronischer Kommunikation genügt hierfür nicht. Wo die Grenze zwischen ausreichender und unzureichender Absicherung verläuft, lässt sich allerdings nicht abstrakt für alle Fallgestaltungen bestimmen. Wird ein Verwaltungsakt über einen ungesicherten Kommunikationsweg übermittelt, lässt sich häufig nicht zuverlässig feststellen, von wem das Dokument tatsächlich stammt oder ob der angegebene Absender mit der handelnden Person identisch ist. Aus diesem Grund knüpft das staatliche Recht die Anerkennung elektronischer Verfahren an zusätzliche Sicherungen. § 3a Abs. 2 Satz 1 VwVfG erlaubt zwar grundsätzlich den Ersatz der Schriftform durch die elektronische Form. Für bestimmte elektronische Zustellungen verlangt das Verwaltungszustellungsrecht jedoch weitergehende Schutzmechanismen. Das Dokument muss mit einer qualifizierten elektronischen Signatur versehen und gegen die unbefugte Kenntnisnahme Dritter abgesichert sein. Die rechtliche Anerkennung elektronischer Kommunikation erfolgt damit nicht voraussetzungslos, sondern innerhalb geregelter Identifizierungs- und Sicherheitsstrukturen. Die technische Möglichkeit allein reicht daher nicht aus.

Das Kirchliche Datenschutzgesetz knüpft an eine kontrollierte und nachvollziehbare Zuordnung an. Personen, die personenbezogene Daten verarbeiten, sind nach § 5 KDG zur Wahrung des Datengeheimnisses verpflichtet. Zugleich macht § 6 Abs. 1 KDG deutlich, dass die Verarbeitung personenbezogener Daten einer rechtlichen Grundlage bedarf. Digitale Verwaltungsakte setzen daher nicht lediglich einen technischen Übermittlungsvorgang voraus. Sie bewegen sich zugleich innerhalb eines rechtlich geregelten Rahmens der Datenverarbeitung.³⁴ Für die kirchliche Verwaltung bedeutet dies, dass eine elektronische Mitzeichnung oder Freigabe die Funktion der handschriftlichen Mitzeichnung nach c. 474 CIC nur dann erfüllen kann, wenn die handelnde Person eindeutig identifizierbar bleibt und die Erklärung ihr persönlich zugerechnet werden kann. Gerade dieser Gedanke liegt den Vorschriften über qualifizierte elektronische Signaturen zugrunde. Die eIDAS-Verordnung verlangt deshalb Schutzmechanismen, welche die

³³ Siehe: Der Erzbischof von Köln, Gesetz über den kirchlichen Datenschutz (KDG) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017, in: Amtsblatt des Erzbistums Köln, Nr. 12, S. 13-35; zuletzt geändert durch: Gesetz zur Änderung des Gesetzes über den Kirchlichen Datenschutz (KDG) (KDG-Änderungsgesetz), in: Amtsblatt des Erzbistums Köln, Nr. 71, S. 123-143.

³⁴ Die eIDAS-Verordnung bindet elektronische Authentizität an die eindeutige Zuordnung zum Unterzeichner, dessen Identifizierbarkeit sowie die Verbindung der Signatur mit den signierten Daten in einer Weise, dass nachträgliche Veränderungen erkennbar werden (vgl. Art. 26 eIDAS-VO). Damit wird die elektronische Zurechnung rechtlich an persönliche Identität und Integritätsschutz geknüpft. Siehe auch § 33 Abs. 1 Satz 3 BNotO; § 33 Abs. 4 BNotO.

Vertraulichkeit der Signaturerstellungsdaten sichern und ihre missbräuchliche Verwendung verhindern sollen.³⁵

Mit der Frage der Zurechenbarkeit steht die Authentizität elektronischer Dokumente in engem Zusammenhang. Digitale Dokumente lassen sich ohne Qualitätsverlust vervielfältigen und in unterschiedlichen Versionen speichern. Für kirchliche Verwaltungsakte muss deshalb jederzeit nachvollziehbar bleiben, welches Dokument den maßgeblichen Rechtsakt verkörpert und ob nachträgliche Veränderungen vorgenommen wurden.³⁶ Die Tragfähigkeit digitaler Verwaltungsakte setzt folglich voraus, dass Erstellung, Speicherung und Archivierung innerhalb gesicherter Systeme erfolgen.³⁷

Die Unverändertheit elektronischer Verwaltungsunterlagen bedarf besonderer Sicherungen. Digitale Dokumente können technisch verändert werden, ohne dass dies äußerlich sofort erkennbar wäre. Deshalb müssen elektronische Akten organisatorisch und technisch zuverlässig abgesichert werden. Ebenso kennt das kirchliche Recht diesen Gedanken. Die Archivvorschriften der cc. 486-489 CIC beschränken sich nicht darauf, die bloße Aufbewahrung von Dokumenten anzuordnen. Verlangt werden vielmehr eine geordnete Verwahrung, geregelte Zugangsbedingungen sowie besondere Schutzvorkehrungen für vertrauliche und geheime Unterlagen. Nach c. 486 § 1 CIC sind die Dokumente der Diözese mit größter Sorgfalt aufzubewahren. C. 487 CIC regelt den Zugang zum Archiv, während c. 489 CIC besondere Sicherungen für geheime Archivbestände vorsieht. Dahinter steht die Vorstellung, dass kirchliche Verwaltungsunterlagen nach längerer Zeit noch in einer Form vorhanden sein müssen, die eine zuverlässige Feststellung ihres Inhalts und ihres rechtlichen Zusammenhangs ermöglicht.

Im digitalen Umfeld stellt sich dieses Erfordernis auf andere Weise. Elektronische Verwaltungssysteme müssen gewährleisten, dass Änderungen nachvollziehbar bleiben, Zugriffe dokumentiert werden und frühere Bearbeitungsstände bei Bedarf rekonstruiert werden können. Welche konkreten Anforderungen hierfür erforderlich sind, hängt wesentlich von Art, Bedeutung und Sensibilität des jeweiligen Verwaltungsvorgangs ab. Hier setzen die Vorgaben des Kirchlichen Datenschutzgesetzes an. § 26 Abs. 1 KDG verlangt ausdrücklich „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Nicht die Technik als solche ist entscheidend, sondern ob die rechtlichen Sicherungsfunktionen durch die konkrete organisatorische und technische Ausgestaltung gewährleistet werden.³⁸ § 27 KDG verlangt bereits bei der Gestaltung von Verarbeitungssystemen datenschutzgerechte Voreinstellungen und technische Schutzmaßnahmen.³⁹ Dass es hierbei nicht lediglich um Fragen technischer Speicherung geht, zeigt das Notarrecht. Nach § 35 Abs. 1 Satz 1 BNotO sind notarielle Akten und Verzeichnisse so zu führen, dass ihre Verfügbarkeit, Integrität, Transparenz und Vertraulichkeit gewährleistet bleiben. Der Wortlaut beschreibt damit Anforderungen, die weit über eine bloße elektronische Ablage hinausgehen. Aktenführung bedeutet zugleich Bestandssicherung, Nachvollziehbarkeit

³⁵ Vgl. Anhang II Nr. 1 Buchst. d eIDAS-VO.

³⁶ Vgl. c. 51 CIC; c. 486 §1 CIC.

³⁷ Vgl. c. 474 CIC; c. 486 §1 CIC.

³⁸ Der Gesetzgeber nennt ausdrücklich Maßnahmen zur Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sowie Verfahren zur regelmäßigen Überprüfung der Wirksamkeit dieser Schutzmaßnahmen.

³⁹ Damit wird deutlich, dass digitale Verwaltung rechtlich nicht bloß elektronische Ablage bedeutet, sondern eine kontrollierte und überprüfbare Informationsverarbeitung voraussetzt.

des Verwaltungsvorgangs, Schutz vor unbefugten Veränderungen und eine Beschränkung des Zugriffs auf berechtigte Personen. Für kirchliche Verwaltungsakten liegt dieser Vergleich nahe, weil sie nicht lediglich einzelne Dokumente enthalten, sondern den rechtlich erheblichen Zusammenhang kirchlichen Verwaltungshandelns festhalten.

Eigenständige Anforderungen ergeben sich für die Mitteilung elektronischer Verwaltungsakte. Nach c. 54 CIC entfaltet ein Dekret seine rechtliche Wirkung grundsätzlich erst mit seiner rechtmäßigen Mitteilung. Zugang und Kenntnismöglichkeit gehören daher selbst zu den rechtlich relevanten Voraussetzungen des Verwaltungsvorgangs. Während sich der Zugang eines eingeschriebenen Briefes meist vergleichsweise leicht dokumentieren lässt, können bei elektronischen Kommunikationsformen andere Schwierigkeiten entstehen. Das staatliche Verwaltungsrecht misst dieser Frage erhebliche Bedeutung bei. Nach § 2 Abs. 1 VwZG ist unter Zustellung die Bekanntgabe eines schriftlichen oder elektronischen Dokuments in der gesetzlich vorgesehenen Form. Hinzu tritt § 5 Abs. 7 Satz 5 VwZG, der die Dokumentation des Übermittlungszeitpunkts und des verwendeten Zugangs vorsieht. Der Nachweis des Zugangs erscheint damit nicht als bloße technische Nebenfrage, sondern als eigenständiger Bestandteil der rechtlichen Verlässlichkeit elektronischer Verwaltungsverfahren.⁴⁰

Die langfristige Archivierung wirft im digitalen Umfeld zusätzliche Schwierigkeiten auf. Kirchliche Archive dienen nicht allein administrativen Zwecken. Sie sichern zugleich die dauerhafte Nachweisbarkeit kirchlicher Rechtsverhältnisse und bilden damit einen wesentlichen Bestandteil rechtlicher Kontinuität. Die Lesbarkeit elektronischer Dokumente hängt von Dateiformaten, Speichersystemen und der jeweiligen technischen Infrastruktur ab. Während papiergebundene Unterlagen häufig über Jahrzehnte hinweg ohne besondere Hilfsmittel lesbar bleiben, erfordern digitale Akten eine fortlaufende technische Betreuung und Sicherung. Bereits die kirchlichen Archivvorschriften verstehen Archivierung nicht als bloße Aufbewahrung. C. 486 CIC verlangt eine geordnete und sorgfältige Verwahrung der Dokumente der Diözese. Dahinter steht nicht lediglich das Interesse an historischer Dokumentation. Die Regelung dient ebenso der dauerhaften Sicherung rechtlich relevanter Unterlagen. Elektronische Archivierung verlangt deshalb stabile Speicherstrukturen, geregelte Zugriffsrechte und Dokumentenformate, die langfristig nutzbar bleiben.

Das Kirchliche Datenschutzgesetz nimmt diese Archivfunktion ausdrücklich auf. Nach § 31 KDG haben Verantwortliche ein Verzeichnis ihrer Verarbeitungstätigkeiten zu führen. § 35 KDG verlangt bei Verarbeitungsvorgängen mit voraussichtlich hohem Risiko die Durchführung einer Datenschutz-Folgenabschätzung. Hinzu treten besondere Regelungen für Archivzwecke in §§ 19 Abs. 3 lit. d, 20 Abs. 4 und 22 Abs. 5 KDG. Danach können Ansprüche auf Löschung, Einschränkung der Verarbeitung oder Datenübertragbarkeit zurücktreten, soweit ihre Wahrnehmung kirchliche Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen würde. Archivierung dient nicht lediglich der Speicherung von Daten, sondern erfüllt eine eigenständige Dokumentations- und Beweisfunktion.

⁴⁰ Die eIDAS-Verordnung behandelt elektronische Zustellung nicht als bloßen Versandvorgang. Dienste für die Zustellung elektronischer Einschreiben erbringen nach Art. 3 Nr. 36 eIDAS-VO den Nachweis der Absendung und des Empfangs und schützen die übermittelten Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung. Für qualifizierte Dienste gilt zudem die Vermutung der Integrität der Daten sowie der Absendung durch den identifizierten Absender und des Empfangs durch den identifizierten Empfänger (vgl. Art. 43 Abs. 2 eIDAS-VO). Damit verbindet die Verordnung elektronische Kommunikation ausdrücklich mit Identitätssicherung, Integritätsschutz und Nachweisbarkeit des Zugangs.

Zudem berücksichtigt das europäische Vertrauensdiensterecht die zeitliche Einordnung elektronischer Dokumente. Elektronische Zeitstempel verknüpfen Daten mit einem bestimmten Zeitpunkt und ermöglichen deren verlässliche zeitliche Zuordnung. Für qualifizierte elektronische Zeitstempel gilt darüber hinaus die Vermutung der Richtigkeit von Datum und Uhrzeit sowie der Unversehrtheit der damit verbundenen Daten. Die rechtliche Bedeutung elektronischer Dokumente beschränkt sich damit nicht auf den Zeitpunkt ihrer Erstellung. Ebenso wichtig bleibt die Möglichkeit, ihre Existenz und ihren Zustand nach längerer Zeit zuverlässig nachweisen zu können.⁴¹ Das Elektronische Urkundenarchiv des Notariats zeigt, dass diese Anforderung praktisch umgesetzt werden kann. Nach § 78h Abs. 2 Satz 1 BNotO müssen Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit und Transparenz der gespeicherten Daten während der gesamten Aufbewahrungsfrist gewährleistet bleiben. Die Urkundenarchivbehörde hat hierzu die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um den Beweiswert der verwahrten elektronischen Dokumente dauerhaft zu erhalten.⁴² Digitale Archivierung geht daher über die bloße Speicherung eines Dokuments hinaus. Entscheidend bleibt vielmehr, dass die verlässliche Zuordnung eines Verwaltungsvorgangs auch nach vielen Jahren noch erhalten bleibt. Darin liegt eine zentrale Herausforderung moderner Verwaltungsorganisation, nicht nur im staatlichen, sondern ebenso im kirchlichen Bereich.

5 Anwendung auf den *actus administrationis*

Nachdem die Anforderungen an Verwaltungsakte im engeren Sinne dargestellt wurden, richtet sich die Untersuchung nun auf die sonstigen Akte der kirchlichen Verwaltung. Hierzu zählen insbesondere notarielle Beurkundungen, Protokolle, Registereinträge, interne Verwaltungsvorgänge sowie die Führung und Aufbewahrung kirchlicher Archive. Ihr Schwerpunkt liegt in der Dokumentation, Registrierung und Sicherung kirchlicher Verwaltungsvorgänge.⁴³ Die Herausforderungen der Digitalisierung betreffen in diesem Bereich daher vor allem die Frage, ob Authentizität, Integrität, Nachvollziehbarkeit und Verfügbarkeit kirchlicher Dokumentation sowie deren datenschutzrechtlich ordnungsgemäße Verarbeitung dauerhaft gewährleistet werden können.⁴⁴

Die einschlägigen kanonischen Vorschriften betreffen vor allem die Tätigkeit kirchlicher Notare sowie die Ordnung der kirchlichen Archive. Nach c. 474 CIC müssen Akte der Kurie, die rechtliche Wirkung entfalten sollen, vom Ordinarius unterzeichnet und vom Kanzler oder einem Notar gegengezeichnet werden. Die Mitunterzeichnung erschöpft sich dabei nicht in einer verwaltungsinternen Ordnungsvorschrift. Sie dient der Authentizität des Dokuments und seiner Zuordnung zum zuständigen Amtsträger. Die cc. 482-484 CIC konkretisieren diese Aufgabe, indem sie dem Kanzler und den Notaren die Ausfertigung, Dokumentation und Verwahrung kirchlicher Akten übertragen. Die Archivvorschriften der cc. 486-491 CIC verlangen ergänzend die geordnete und sichere Führung kirchlicher Archive. Im Zusammenhang gelesen schützen

⁴¹ Vgl. Art. 3 Nr. 33; Art. 41 Abs. 2 eIDAS-VO.

⁴² Vgl. § 78h Abs. 2 Satz 2 BNotO.

⁴³ Vgl. c. 482 §1 CIC; c. 486 §1 CIC.

⁴⁴ Vgl. § 26 Abs. 1 KDG; § 27 Abs. 1 KDG.

diese Normen nicht nur den Inhalt kirchlicher Verwaltungsvorgänge. Ebenso bedeutsam sind deren zuverlässige Dokumentation und spätere Nachweisbarkeit.

Zu prüfen ist daher, ob digitale Systeme Dokumente ebenso zuverlässig erfassen, sichern und verfügbar halten können wie die herkömmliche papiergebundene Verwaltung. Gerade weil die hier behandelten Vorgänge regelmäßig keine eigenständige rechtsgestaltende Wirkung entfalten, begegnet ihre Digitalisierung grundsätzlich geringeren rechtlichen Schwierigkeiten als die elektronische Form eines Dekrets oder sonstigen Verwaltungsaktes mit unmittelbarer Rechtswirkung. Ihre Funktion besteht vor allem darin, Verwaltungsvorgänge zu dokumentieren, deren rechtliche Bedeutung an anderer Stelle entsteht. Elektronische Systeme können diese Funktion erfüllen, wenn sie die zuvor herausgearbeiteten Sicherungszwecke in der dokumentierenden Verwaltung wahren.⁴⁵

Bei Register- und Aktenführung verstehen moderne Rechtsordnungen elektronische Dokumentation nicht als bloße Ablage einzelner Dateien. Das Bundesdatenschutzgesetz verlangt für bestimmte Verarbeitungskontexte die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, das unter anderem Zwecke der Verarbeitung, Kategorien betroffener Personen und Daten, Empfänger sowie technische und organisatorische Maßnahmen ausweisen muss.⁴⁶ Das E-Government-Gesetz (EGovG) formuliert diesen Ansatz noch deutlicher.⁴⁷ § 6a Satz 1 EGovG bestimmt: „Die Behörden des Bundes sollen ihre Akten elektronisch führen.“ Wird eine Akte elektronisch geführt, ist nach § 6a Satz 3 EGovG durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden. Diese Vorschriften gelten zwar nicht unmittelbar für die kirchliche Verwaltung. Ihnen liegt jedoch ein Rechtsgedanke zugrunde, der sich den Archivvorschriften des Codex entnehmen lässt. Aktenführung erschöpft sich nicht in der Aufbewahrung von Dokumenten. Sie setzt vielmehr eine geordnete, nachvollziehbare und dauerhaft gesicherte Verwaltung von Informationen voraus.⁴⁸

Die Bundesnotarordnung bestätigt diesen Ansatz in einem besonders formgebundenen Bereich staatlicher Verwaltung. Nach § 35 Abs. 1 Satz 1 BNotO sind notarielle Akten und Verzeichnisse so zu führen, „dass deren Verfügbarkeit, Integrität, Transparenz und Vertraulichkeit gewährleistet sind“. Zugleich erlaubt § 35 Abs. 2 Satz 1 BNotO die Führung von Akten und Verzeichnissen in Papierform oder elektronisch, soweit die Form nicht durch oder aufgrund eines Gesetzes vorgeschrieben ist.⁴⁹ Das Bundesarchivgesetz (BArchG)⁵⁰ knüpft die

⁴⁵ Ein staatlicher Vergleichspunkt findet sich in § 33 Abs. 4 VwVfG, das die Beglaubigung bei Ausdrucken elektronischer Dokumente und bei elektronischen Dokumenten vorsieht (siehe § 33 Abs. 4 Nr. 3 und 4 VwVfG). Sie verdeutlicht damit, dass elektronische Dokumente nicht schon wegen ihrer technischen Form aus dem Bereich amtlicher Dokumentation ausscheiden.

⁴⁶ Vgl. § 70 Abs. 1 BDSG.

⁴⁷ Siehe Gesetz zur Förderung der elektronischen Verwaltung (E-Government Gesetz - EGovG) vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 11 des Gesetzes vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301) geändert worden ist.

⁴⁸ § 26 Abs. 1 KDG verpflichtet Verantwortliche und Auftragsverarbeiter zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein angemessenes Schutzniveau zu gewährleisten. Hierzu gehören insbesondere Maßnahmen zur Sicherung von Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitungssysteme. Ergänzend verlangt § 27 Abs. 1 KDG die Berücksichtigung datenschutzfreundlicher Technikgestaltung und Voreinstellungen bereits bei der Ausgestaltung der Systeme.

⁴⁹ Damit wird die elektronische Aktenführung nicht als bloße technische Ablage verstanden, sondern an konkrete Sicherungsfunktionen gebunden. Für kirchliche Verwaltungsdokumentation ist dies ein wichtiger Vergleichspunkt, weil dort nicht das Speichermedium, sondern die geordnete und geschützte Führung des Verwaltungsvorgangs ausschlaggebend ist.

⁵⁰ Siehe Gesetz über die Nutzung und Sicherung von Archivgut des Bundes (Bundesarchivgesetz - BArchG) in der Fassung der Bekanntmachung vom 6. September 2021 (BGBl. I S. 4122), das durch Artikel 26 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2759) geändert worden ist.

Archivfähigkeit von Unterlagen nicht an deren Speicherform, sondern an ihre dauerhafte Sicherung und Nutzbarkeit.⁵¹ Für kirchliche Archive besitzen diese Vorschriften keine unmittelbare Geltung. Sie verweisen jedoch auf einen archivrechtlichen Grundgedanken, der über die einzelnen Rechtsordnungen hinausreicht: Elektronische Unterlagen müssen dauerhaft gesichert, zugänglich gehalten und vor Verlust oder unkontrollierter Veränderung geschützt werden.

Im Rahmen der digitalen notariellen Dokumentation besteht die Aufgabe des kirchlichen Notars nicht darin, lediglich einen äußeren Formalakt vorzunehmen. Er sichert vielmehr die Echtheit eines Dokuments und dessen ordnungsgemäße Einbindung in den Verwaltungsvorgang. Der Codex verbindet die notarielle Tätigkeit damit erkennbar mit persönlicher Vertrauenswürdigkeit und amtlicher Verlässlichkeit. In einer elektronischen Umgebung muss deshalb feststehen, welche Person die notarielle Funktion ausgeübt hat, wann diese Mitwirkung erfolgt ist und auf welches Dokument sie sich bezieht. Ebenso wichtig ist die Möglichkeit festzustellen, ob der Inhalt nachträglich verändert wurde. Eine elektronische notarielle Dokumentation kann diese Funktion erfüllen, wenn sie innerhalb eines geschützten Verwaltungssystems erfolgt und die notarielle Mitwirkung dauerhaft nachvollziehbar bleibt.⁵² Das staatliche Notarrecht bindet elektronische Mitwirkung an persönliche Zurechenbarkeit und technische Absicherung. Die elektronische Form wird nur anerkannt, wenn die notarielle Mitwirkung eindeutig dem Amtsträger zugeordnet und dauerhaft überprüfbar bleibt.⁵³ Darin liegt ein aufschlussreicher Vergleichspunkt für die digitale kirchliche Notariatsfunktion.

Vergleichbare Überlegungen gelten für Register und Archive. Die kirchlichen Archivnormen verlangen geordnete Aufbewahrung, Schutz vor Verlust und unbefugtem Zugriff sowie zuverlässige Wiederauffindbarkeit der Dokumente. Nach c. 487 § 1 CIC muss das Archiv verschlossen bleiben; allein der Bischof und der Kanzler dürfen den Schlüssel besitzen. Bereits diese Norm zeigt, dass Zugangsschutz und kontrollierte Verwahrung zu den grundlegenden Strukturprinzipien kirchlicher Archivführung gehören. Digitale Archivsysteme können diesen Anforderungen entsprechen, sofern sie dauerhafte Speicherung, kontrollierte Zugriffsrechte, Protokollierung und langfristige Lesbarkeit sicherstellen.⁵⁴ Einen hilfreichen Vergleich bietet dabei § 7 Abs. 1 Satz 2 EGovG für die Übertragung vorhandener Papierdokumente in elektronische Akten. Danach ist bei der Übertragung nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.⁵⁵ Zusätzlich enthält § 5 Abs. 3 BArchG Hinweise für die elektronische Archivierung. Werden elektronische Unterlagen dem Bundesarchiv angeboten, richten sich Form der Übermittlung und Datenformat nach verbindlichen Standards der Bundesverwaltung.⁵⁶ Fehlt ein solcher Standard, sind Form und Format im Einvernehmen mit der abgebenden Stelle festzulegen.⁵⁷ Digitale

⁵¹ § 1 Nr. 10 BArchG. Zugleich beschreibt § 3 Abs. 1 Satz 1 BArchG die Aufgabe des Bundesarchivs dahin, „das Archivgut des Bundes auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten“.

⁵² Vgl. c. 474 CIC; c. 484 CIC.

⁵³ Vgl. § 33 Abs. 1 Satz 3 BNotO.

⁵⁴ Vgl. § 78h Abs. 2 Satz 1 BNotO. Danach müssen Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit und Transparenz der verwahrten elektronischen Dokumente während der gesamten Aufbewahrungsfrist gewährleistet sein.

⁵⁵ Vgl. § 371b ZPO zur Beweiskraft elektronischer Dokumente, die nach dem Stand der Technik aus öffentlichen Urkunden übertragen wurden.

⁵⁶ Vgl. § 5 Abs. 3 Satz 1 BArchG.

⁵⁷ Vgl. § 5 Abs. 3 Satz 2-3 BArchG.

Verwaltungsdokumente müssen daher von Anfang an in Formaten und Ordnungssystemen geführt werden, die ihre spätere Sicherung, Nutzung und Überprüfung ermöglichen.⁵⁸

Ein Protokoll einer Sitzung des Diözesanverwaltungsrates kann daher elektronisch geführt und archiviert werden, wenn seine Erstellung nachvollziehbar dokumentiert, der Zugriff beschränkt und spätere Veränderungen ausgeschlossen oder eindeutig protokolliert werden. Rechtlich unzureichend wäre dagegen eine Ablage in frei bearbeitbaren Dateien ohne Zugriffskontrolle, Versionierung und gesicherte Archivierungsstruktur. Bei personenbezogenen Daten tritt hinzu, dass Löschung, Einschränkung der Verarbeitung und Aufbewahrungspflichten systematisch miteinander abgestimmt werden müssen.⁵⁹ Für elektronische Unterlagen führt das BArchG diesen Gedanken weiter. Nach § 5 Abs. 3 Satz 4 BArchG hat die anbietende öffentliche Stelle nach Ablauf der Aufbewahrungsfrist verbliebene Kopien elektronischer Unterlagen nach dem Stand der Technik zu löschen, wenn der bleibende Wert festgestellt und die Übernahme erfolgt ist; über die Löschung ist ein Nachweis zu fertigen. Archivierung erschöpft sich damit nicht in der bloßen Vervielfältigung von Unterlagen. Sie verlangt vielmehr eine kontrollierte Entscheidung darüber, welche Fassung dauerhaft gesichert wird und welche Kopien nach rechtlichen Maßstäben zu beseitigen sind.⁶⁰ Die BNotO verfolgt für die elektronische Dokumentation einen vergleichbaren Ansatz. Der Zugang zum Elektronischen Urkundenarchiv steht nach § 78i BNotO ausschließlich der für die Verwahrung zuständigen Stelle zu. Zugleich zeigt § 51a Abs. 1 Satz 1 BNotO für den Fall des Erlöschens des Amtes, dass nicht nur papiergebundene Akten und Verzeichnisse abzuliefern sind, sondern der Zugang zu elektronisch geführten Akten und Verzeichnissen zu ermöglichen ist. Daraus ergeben sich Gesichtspunkte für die kirchliche Verwaltung. Elektronische Aktenführung muss Zuständigkeitswechsel, Verwahrung, spätere Einsicht und institutionelle Kontinuität rechtlich beherrschbar machen. Im Bereich der Diözesankurie setzt dies voraus, dass elektronische Akten nicht an einzelne Personen oder private Systeme gebunden bleiben, sondern institutionell kontrolliert verwaltet werden.

Insgesamt spricht vieles dafür, dass die Digitalisierung eines *actus administrationis* mit den Anforderungen des kanonischen Rechts vereinbar wäre. Ihre Zulässigkeit hängt jedoch davon ab, ob die dokumentierende, authentifizierende, datenschutzrechtliche und archivierende Funktion dieser Akte zuverlässig gewahrt bleibt. Wo digitale Systeme eindeutige Zuordnung, gesicherte Integrität, geordnete Zugriffsmöglichkeiten, dauerhafte Verfügbarkeit, kontrollierte Verarbeitung personenbezogener Daten, standardisierte Übergabefähigkeit und eine rechtlich kontrollierte Aktenführung gewährleisten, können sie die Zwecke kirchlicher Verwaltungsdokumentation erfüllen. Fehlen diese Voraussetzungen, bleibt die digitale Form rechtlich unzureichend.

⁵⁸ Vgl. c. 486 CIC; c. 487 §1 CIC.

⁵⁹ § 19 KDG gewährt grundsätzlich ein Recht auf Löschung personenbezogener Daten, sieht jedoch Ausnahmen für im kirchlichen Interesse liegende Archivzwecke vor, soweit eine Löschung deren Verwirklichung unmöglich machen oder ernsthaft beeinträchtigen würde (vgl. § 19 Abs. 4 lit. d KDG). Entsprechendes gilt für das Recht auf Einschränkung der Verarbeitung nach § 20 Abs. 4 KDG. Das KDG trägt damit der besonderen Funktion kirchlicher Archive für Dokumentation und Nachweisbarkeit Rechnung.

⁶⁰ Vgl. § 35 Abs. 6 BNotO; § 8 EGovG; § 5 Abs. 7 Satz 5 VwZG; sie betreffen die archivische Übernahme oder Löschung elektronischer Akten, die Bereitstellung elektronischer Akteninhalte sowie die Dokumentation elektronischer Übermittlungsvorgänge.

6 Anwendung auf den *actus administrativus*

Noch deutlicher treten die Digitalisierungsfragen bei Verwaltungsakten im engeren Sinne hervor. Der Grund liegt in ihrer unmittelbaren Rechtswirkung. Ein Dekret, ein Reskript, eine Ernennung oder eine sonstige Verwaltungsentscheidung hält nicht nur Verwaltungshandeln fest, sondern kann innerhalb der kirchlichen Rechtsordnung konkrete Rechte und Pflichten begründen, verändern oder beenden.⁶¹ Die Anforderungen an Form, Authentizität und Mitteilung betreffen daher nicht nur die äußere Gestalt des Dokuments, sondern die rechtliche Absicherung des Verwaltungsaktes selbst. Zusätzlich sind datenschutzrechtliche Anforderungen zu berücksichtigen, weil Verwaltungsakte regelmäßig personenbezogene Daten enthalten und deshalb nicht nur rechtmäßig erlassen, sondern kontrolliert verarbeitet, gespeichert und übermittelt werden müssen.⁶²

Aufbauend auf den zuvor entwickelten Auslegungsgrundsätzen sind die Anforderungen an den *actus administrativus* gesondert zu betrachten. Die cc. 35-93 CIC enthalten hierfür den maßgeblichen Rechtsrahmen. Für Einzeldekrete sind insbesondere die cc. 48-58 CIC maßgeblich. Besondere Bedeutung kommt c. 51 CIC zu. Danach soll ein Dekret schriftlich erlassen werden und, wenn es sich um eine Entscheidung handelt, wenigstens summarisch die Entscheidungsgründe enthalten. Die Schriftlichkeit dient dabei nicht bloß der Fixierung des Inhalts. Der Verfasser ist der Meinung, dass gerade c. 51 CIC zeigt, dass der Gesetzgeber die Nachvollziehbarkeit administrativer Entscheidungen stärker betont als das verwendete Trägermedium. Sie gewährleistet Rechtssicherheit, Nachprüfbarkeit und die Möglichkeit, den Verwaltungsakt gegebenenfalls im hierarchischen Rekurs anzugreifen. Dies gilt in gleicher Weise für digitale Verwaltungsverfahren.⁶³ Herkunft, Inhalt und rechtlich maßgeblicher Zeitpunkt müssen verlässlich feststehen. Die traditionelle kirchliche Verwaltung sichert diese Funktionen insbesondere durch Unterzeichnung, amtliche Dokumentation und die Mitwirkung des Kanzlers oder eines Notars gemäß c. 474 CIC. Dadurch bleiben Herkunft, Authentizität und Nachweisbarkeit des Verwaltungsaktes gewährleistet.

Digitale Dokumente können diese Funktionen grundsätzlich ebenfalls erfüllen, sofern sie nicht lediglich als frei bearbeitbare Dateien behandelt werden. Erforderlich bleibt ein gesicherter Zusammenhang von Erstellung, Signatur und Archivierung. Der erlassende Amtsträger muss erkennbar bleiben, der Inhalt darf nicht unbemerkt verändert werden können, und der Verwaltungsakt muss später zuverlässig rekonstruierbar sein. Das staatliche Recht erkennt die elektronische Form als funktionalen Ersatz der Schriftform an, sofern Identifizierbarkeit, Integrität und Nachweisbarkeit der Erklärung gewährleistet bleiben. Dies zeigen insbesondere § 37 Abs. 3 Satz 1 VwVfG sowie §§ 126 Abs. 3, 126a Abs. 1 BGB.⁶⁴ C. 474 CIC verlangt die Unterzeichnung durch den Ordinarius sowie die Mitunterzeichnung durch den Kanzler oder

⁶¹ Vgl. cc. 35, 48 CIC.

⁶² Vgl. §§ 6-7, 26 KDG.

⁶³ Vgl. cc. 1732-1739 CIC.

⁶⁴ Die eIDAS-Verordnung verlangt für fortgeschrittene elektronische Signaturen insbesondere die eindeutige Zuordnung zum Unterzeichner, dessen Identifizierbarkeit sowie die Erkennbarkeit nachträglicher Veränderungen der signierten Daten (vgl. Art. 26 eIDAS-VO). Vergleichbar bindet § 33 Abs. 1 und 4 BNotO elektronische Signaturen an die persönliche Amtsausübung des Notars. Für kirchliche Verwaltungsakte ergibt sich daraus, dass elektronische Mitzeichnungen nur dann funktional gleichwertig sind, wenn sie persönlich zurechenbar bleiben.

einen Notar. Der Norm lässt sich jedoch nicht entnehmen, dass diese Anforderungen zwingend an eine papiergebundene Ausfertigung anknüpfen.

Die institutionelle Herkunft eines Dokuments kann elektronisch gesichert werden. Nach der hier vertretenen Auffassung bestehen hinreichende Gründe, die institutionelle Authentifizierung nicht auf papiergebundene Verfahren zu beschränken. Art. 3 Nr. 25 eIDAS-VO definiert elektronische Siegel als Daten, die mit anderen elektronischen Daten verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. Für qualifizierte elektronische Siegel gilt nach Art. 35 Abs. 2 eIDAS-VO die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe. Dadurch kann nicht nur die persönliche Unterzeichnung, sondern die institutionelle Zuordnung eines kirchlichen Verwaltungsaktes abgesichert werden. Für die digitale Ausfertigung eines Dekrets folgt daraus, dass die elektronische Form allein nicht ausschlaggebend ist. Zentral ist, ob die Funktionen des schriftlichen Verwaltungsaktes gewahrt bleiben. Wird ein Dekret innerhalb eines geschützten Verwaltungssystems erstellt, eindeutig dem zuständigen Ordinarius zugeordnet, unveränderbar gespeichert und geordnet archiviert, kann die Schriftlichkeit funktional erhalten bleiben. Ein qualifiziertes elektronisches Siegel kann als Beispiel dafür dienen, wie die institutionelle Herkunft eines Dokuments technisch abgesichert werden könnte. Fehlen dagegen Zugriffsschutz, Protokollierung, Versionierung oder eine gesicherte Archivierungsstruktur, bleibt die elektronische Form rechtlich unzureichend.⁶⁵

Die Verarbeitung personenbezogener Daten unterliegt darüber hinaus den Vorgaben des KDG. § 26 Abs. 1 KDG verpflichtet Verantwortliche und Auftragsverarbeiter, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Regelung nennt insbesondere die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sowie Verfahren zur regelmäßigen Überprüfung der Wirksamkeit dieser Maßnahmen.⁶⁶ Für digitale Verwaltungsakte gewinnt dies besondere Bedeutung, weil ihre rechtliche Verlässlichkeit davon abhängt, dass Inhalt, Aussteller und Schutz vor unbefugter Veränderung dauerhaft gesichert bleiben. Elektronische Verwaltungsakte benötigen daher nicht nur eine formale Signatur, sondern zugleich technisch kontrollierte Verwaltungs- und Speicherstrukturen.⁶⁷

Von zentraler Bedeutung ist zudem die rechtmäßige Mitteilung. Nach c. 54 § 1 CIC entfaltet ein Dekret grundsätzlich erst mit rechtmäßiger Mitteilung seine Wirkung.⁶⁸ Elektronische Mitteilungssysteme können diese Anforderungen nur erfüllen, wenn sie Zugang, Empfangszeitpunkt und Empfängeridentität nachvollziehbar dokumentieren. Das Verwaltungszustellungsgesetz konkretisiert diesen Gedanken für elektronische Zustellungen. Nach § 5 Abs. 7 Satz 1 VwZG genügt zum Nachweis der Zustellung ein mit Datum und Unterschrift versehenes Empfangsbekenntnis, das elektronisch zurückgesandt werden kann. Zudem verlangt § 5 Abs. 7 Satz 5 VwZG, dass Zeitpunkt und Zugang der elektronischen Übermittlung aktenkundig

⁶⁵ Vgl. c. 474 CIC; c. 486 §1 CIC; § 26 Abs. 1 KDG.

⁶⁶ Vgl. § 26 Abs. 1 lit. b-d KDG.

⁶⁷ Vgl. § 26 Abs. 1 KDG; § 27 Abs. 1 KDG. Ergänzend verpflichtet § 27 KDG zur datenschutzgerechten Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen. Elektronische Verwaltungsverfahren müssen daher bereits ihrer technischen Struktur nach auf kontrollierte Datenverarbeitung und Zugriffsbeschränkung ausgelegt sein.

⁶⁸ Das staatliche Verwaltungsrecht knüpft die Wirksamkeit eines Verwaltungsaktes an seine Bekanntgabe (§ 43 Abs. 1 Satz 1 VwVfG). In beiden Rechtsordnungen setzt die Wirksamkeit eines Verwaltungsaktes damit eine geordnete und nachweisbare Mitteilung voraus. Nach § 130 Abs. 1 Satz 1 BGB wird eine Erklärung gegenüber Abwesenden erst mit ihrem Zugang wirksam. Im staatlichen Recht hängt die Wirksamkeit damit nicht allein von der Erstellung, sondern vom nachweisbaren Zugang ab.

gemacht werden. Die Vertrauenswürdigkeit elektronischer Mitteilungen hängt daher nicht allein vom Versand ab. Ebenso muss ihr Zugang später zuverlässig nachgewiesen werden können.⁶⁹

Verwaltungsakte müssen nicht nur formgerecht erlassen und mitgeteilt werden. Datenschutzrechtliche Vorgaben sind zudem zu beachten. Verwaltungsakte enthalten regelmäßig personenbezogene Daten und müssen daher nicht nur wirksam, sondern vertraulich und zweckgebunden verarbeitet werden. Maßgeblich sind insbesondere die Grundsätze des § 7 KDG sowie die technischen und organisatorischen Anforderungen des § 26 KDG.⁷⁰ Zugleich setzt § 6 Abs. 1 KDG eine Rechtsgrundlage für die Verarbeitung voraus. Die elektronische Verwaltungsentscheidung darf daher nicht zu einer sachfremden oder unbegrenzten Weiterverarbeitung personenbezogener Daten führen.⁷¹

Hierin unterscheidet sich der *actus administrativus* wesentlich vom *actus administrationis*. Während bei Verwaltungsakten vor allem Dokumentation und Archivierung im Vordergrund stehen, betrifft der *actus administrativus* unmittelbar die Setzung kirchlicher Rechtswirkungen. Elektronische Verfahren können in diesem Bereich eingesetzt werden, wenn sie Schriftlichkeit, persönliche und institutionelle Zurechnung, Integrität, Nachweisbarkeit der Mitteilung, Datenschutz und dauerhafte Archivfähigkeit zuverlässig gewährleisten. Fehlen diese Voraussetzungen, kann die elektronische Form den Anforderungen kirchlicher Verwaltungsakte nicht genügen.

7 Technische Mittel zur Sicherung digitaler Verwaltungsakte

Werden kirchliche Verwaltungsakte und Verwaltungsdokumente elektronisch erstellt, übermittelt oder archiviert, erscheint problematisch, durch welche technischen und organisatorischen Mittel die rechtlichen Anforderungen des kirchlichen Verwaltungsrechts gewahrt werden können. Die verwendete Technologie als solche rückt nicht ins Zentrum der Untersuchung, sondern die Diskussion, ob die vom kanonischen Verwaltungsrecht vorausgesetzten Sicherungsfunktionen zuverlässig gewährleistet werden können. Dazu gehören die bereits herausgearbeiteten Anforderungen an Zurechnung, Integrität, Mitteilung, Archivierung und Datenschutz.⁷² Elektronische Signaturen, elektronische Siegel, Zeitstempel, gesicherte Kommunikationssysteme und revisionssichere Archive besitzen deshalb im kirchlichen Recht keine eigenständige sakramental- oder verfassungsrechtliche Bedeutung. Sie sind vielmehr technische Instrumente zur Sicherung jener juristischen Funktionen, die das kanonische Verwaltungsrecht unabhängig vom verwendeten Medium verlangt.⁷³

Die Bedeutung der Authentizität wird besonders deutlich bei der elektronischen Signatur. Kirchliche Verwaltungsakte beruhen auf der Ausübung kirchlicher Leitungsgewalt durch konkrete Amtsträger. Die Ansprüche an Authentizität ergeben sich im kirchlichen Verwaltungsrecht insbesondere aus der persönlichen Verantwortlichkeit des zuständigen

⁶⁹ Qualifizierte elektronische Einschreibedienste gewährleisten nach Art. 43 Abs. 2 eIDAS-VO insbesondere die Nachweisbarkeit von Absendung und Empfang. § 78n BNotO zeigt, dass elektronische Kommunikation in rechtlich gesicherten Verwaltungsstrukturen erfolgen muss.

⁷⁰ Vgl. § 7 Abs. 1 lit. b und f KDG; § 26 Abs. 1 KDG.

⁷¹ Vgl. § 35 Abs. 1 Satz 1 BNotO; § 26a BNotO. Hier wird verdeutlicht, dass elektronische Verwaltungsstrukturen nur innerhalb gesicherter Organisations- und Verantwortungsstrukturen rechtlich tragfähig sind.

⁷² Vgl. c. 35 CIC; c. 54 §1 CIC; § 26 Abs. 1 KDG.

⁷³ Vgl. Art. 3 Nr. 10, 25, 33 und 36 eIDAS-VO.

Amtsträgers sowie aus den Anforderungen des c. 474 CIC an die amtliche Mitwirkung des Kanzlers oder Notars. Elektronische Signaturen können diese Funktion grundsätzlich erfüllen, wenn sie eine eindeutige Identifizierung der handelnden Person ermöglichen und gegen missbräuchliche Verwendung gesichert sind. Ein staatlicher Vergleichspunkt findet sich in § 37 Abs. 3 Satz 2 VwVfG. Danach muss ein schriftlicher oder elektronischer Verwaltungsakt die Unterschrift oder Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten. Die Rechtssicherheit eines Verwaltungsaktes bleibt an eine konkret verantwortliche Person gebunden.⁷⁴

Von der persönlichen Authentizität ist die institutionelle Herkunft elektronischer Dokumente zu unterscheiden. Während handschriftliche Unterschriften vor allem die Erklärung einer bestimmten Person absichern, dienen elektronische Siegel primär der Sicherung amtlicher Herkunft und der Integrität eines Dokuments.⁷⁵ Für kirchliche Verwaltungsakte ist dies besonders relevant, weil zahlreiche Verwaltungsdokumente nicht nur persönliche Erklärungen eines Ordinarius enthalten, sondern zugleich als amtliche Akte einer kirchlichen Behörde oder Kurie erkennbar sein müssen. Ein elektronisches Siegel kann daher die institutionelle Herkunft eines bischöflichen Dekrets, einer kurialen Mitteilung oder eines archivierten Verwaltungsdokuments absichern.⁷⁶ Die amtliche Herkunft eines Verwaltungsdokuments bleibt damit im kirchlichen Recht organisatorisch eingebettet und darf nicht auf eine bloße Datei reduziert werden.

Bei elektronischen Dokumenten muss gewährleistet sein, dass ihr Inhalt dauerhaft gesichert bleibt und spätere Änderungen nachvollziehbar dokumentiert werden. Deshalb genügt die bloße Speicherung frei bearbeitbarer Dateien den Anforderungen kirchlicher Verwaltungsdokumentation regelmäßig nicht. Das kirchliche Datenschutzrecht konkretisiert diese Sicherungsanforderungen für elektronische Verwaltungssysteme. Wie bereits dargelegt, haben Verantwortliche und Auftragsverarbeiter nach § 26 Abs. 1 KDG geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen entsprechenden Nachweis führen zu können. Hierzu gehören insbesondere Maßnahmen zur Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der eingesetzten Systeme. Digitale Sicherung kirchlicher Verwaltungsakte ist daher nicht nur eine Frage der Signatur. Sie betrifft das gesamte Verarbeitungssystem, in dem Verwaltungsakte erstellt, gespeichert, übermittelt und archiviert werden.⁷⁷ Vergleichbare Anforderungen finden sich im Bundesdatenschutzgesetz (BDSG) für automatisierte Verarbeitungssysteme. Nach § 64 Abs. 2 Satz 2 Nr. 1 BDSG müssen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der

⁷⁴ Vgl. Art. 25 Abs. 2 und Art. 26 eIDAS-VO; § 33 Abs. 1 und 4 BNotO. Die rechtliche Verlässlichkeit elektronischer Signaturen knüpft an der eindeutigen Zurechenbarkeit zur verantwortlichen Person an und nimmt Bezug auf die Sicherung des Signaturvorgangs.

⁷⁵ Die eIDAS-Verordnung definiert elektronische Siegel in Art. 3 Nr. 25 eIDAS-VO als Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. Für qualifizierte elektronische Siegel gilt nach Art. 35 Abs. 2 eIDAS-VO die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe.

⁷⁶ Vgl. c. 482 §1 CIC; cc. 486-489 CIC.

⁷⁷ Vgl. § 27 Abs. 1-2 KDG. Diese Norm verlangt datenschutzgerechte Technikgestaltung und datenschutzfreundliche Voreinstellungen. Elektronische Verwaltungssysteme müssen daher bereits strukturell auf Zweckbindung, Datenminimierung und kontrollierte Zugriffsrechte ausgerichtet sein.

Verarbeitung auf Dauer sichergestellt werden. § 64 Abs. 3 BDSG nennt hierzu insbesondere Zugangs-, Speicher-, Benutzer- und Zugriffskontrollen.⁷⁸

Eigenständige Anforderungen betreffen die eingesetzten Kommunikationssysteme. Die rechtliche Wirksamkeit vieler Verwaltungsakte hängt von ihrer nachweisbaren Mitteilung ab. Elektronische Kommunikation muss deshalb nicht nur Übermittlung ermöglichen, sondern Zugang, Zeitpunkt und Identität des Empfängers zuverlässig dokumentieren.⁷⁹

Die rechtliche Absicherung digitaler Verwaltungsvorgänge setzt zudem eine nachvollziehbare Protokollierung voraus. § 76 Abs. 1 BDSG verlangt für automatisierte Verarbeitungssysteme insbesondere die Protokollierung von Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung personenbezogener Daten. Eine vergleichbare Nachweisstruktur findet sich im KDG. Nach § 7 Abs. 2 KDG ist der Verantwortliche für die Einhaltung der Datenschutzgrundsätze verantwortlich und muss dies nachweisen können. § 31 KDG verpflichtet zur Führung eines Verzeichnisses aller Verarbeitungstätigkeiten, das unter anderem Zwecke, Kategorien betroffener Personen und Daten, Empfänger, Löschfristen sowie technische und organisatorische Maßnahmen enthält.⁸⁰ Für digitale Verwaltungsakte bedeutet dies, dass nicht nur das Enddokument gesichert sein muss. Der Verarbeitungsvorgang selbst muss rechtlich nachvollziehbar bleiben.

Die revisionssichere elektronische Archivierung bildet schließlich einen weiteren zentralen Baustein. Kirchliche Archive dienen nicht nur administrativen Zwecken, sondern sichern dauerhaft die Nachweisbarkeit kirchlicher Rechtsverhältnisse. Elektronische Archive müssen deshalb gewährleisten, dass Dokumente langfristig lesbar, auffindbar und gegen unbemerkte Veränderung geschützt bleiben. Gerade digitale Langzeitarchivierung ist rechtlich anspruchsvoll, weil technische Formate, Software und Speichermedien fortlaufendem Wandel unterliegen. Das KDG berücksichtigt die archivische Dimension personenbezogener Daten ausdrücklich. § 6 Abs. 3 KDG stellt klar, dass eine Verarbeitung für im kirchlichen Interesse liegende Archivzwecke nicht als Verarbeitung für einen anderen Zweck gilt, sofern keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen. Für digitale Archive bedeutet dies, dass Langzeitsicherung und Datenschutz nicht getrennt werden dürfen. Archivierung setzt vielmehr eine rechtlich geordnete und technisch gesicherte Aufbewahrung voraus. Die eIDAS-Verordnung berücksichtigt die Langzeitbewahrung elektronischer Signaturen und Siegel, damit ihre Echtheit und Unversehrtheit zu einem späteren Zeitpunkt noch nachgewiesen werden können.⁸¹

78 Vgl. § 6a EGovG; § 35 Abs. 1 Satz 1 BNotO; cc. 486-489 CIC. Elektronische Akten- und Archivführung wird in allen drei Regelungsbereichen an die Wahrung von Verfügbarkeit, Integrität, kontrolliertem Zugang und geordneter Dokumentation gebunden.

79 Das Verwaltungsverfahrensgesetz knüpft die Wirksamkeit eines Verwaltungsaktes an seine Bekanntgabe und verpflichtet die Behörde im Streitfall zum Nachweis des Zugangs (vgl. § 43 Abs. 1 Satz 1; § 41 Abs. 2 Satz 3 VwVfG). Für elektronische Zustellungen verlangt § 5 Abs. 7 Satz 5 VwZG die Dokumentation von Zeitpunkt und Zugang der Übermittlung. Vergleichbar sichern qualifizierte elektronische Einschreibedienste nach Art. 43 Abs. 2 eIDAS-VO Integrität, Absender- und Empfängeridentität sowie den Nachweis der Übermittlung. Der gemeinsame Strukturgedanke besteht darin, elektronische Kommunikation rechtlich nachvollziehbar und beweisbar zu gestalten.

80 Vgl. § 31 Abs. 1 KDG.

81 Vgl. Erwägungsgrund 61; Art. 34 und 41 Abs. 2 eIDAS-VO; siehe auch Vertrauensdienstegesetz (VDG) vom 18. Juli 2017 (BGBl. I S. 2745), das zuletzt durch Artikel 28 des Gesetzes vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301) geändert worden ist; hier: § 15 VDG. Elektronische Beweissicherung verlangt nicht nur die Erstellung, sondern die langfristige Erhaltung von Signaturen, Siegeln und Zeitstempeln. Zeitstempel können dabei insbesondere den Nachweis von Zeitpunkt und Integrität eines elektronischen Verwaltungsdokuments unterstützen.

Der Umgang mit Datenschutzverletzungen bildet einen weiteren Bestandteil digitaler Verwaltungsorganisation. Nach § 33 Abs. 1 KDG hat der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich der Datenschutzaufsicht zu melden, wenn diese Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.⁸² Digitale Verwaltungssysteme müssen daher Störungen, unbefugte Zugriffe und Datenverluste nachvollziehbar erfassen und rechtlich beherrschbar machen.

Die genannten technischen Mittel sind daher kein Selbstzweck. Ihre rechtliche Bedeutung liegt allein darin, dass sie die vom kanonischen Verwaltungsrecht geforderten Sicherungsfunktionen in einer digitalen Umgebung unterstützen. Elektronische Signaturen, Siegel, Zeitstempel, Kommunikationsplattformen, Zustelldienste und Archivsysteme sind nur insoweit rechtlich relevant, als sie Authentizität, Integrität, Nachvollziehbarkeit, Vertraulichkeit, Datenschutz, Zugriffskontrolle und dauerhafte Beweisbarkeit kirchlicher Verwaltungsakte zuverlässig gewährleisten können.

8 Datenschutzrechtliche Dimension

Mit der Digitalisierung kirchlicher Verwaltung gewinnen datenschutzrechtliche Fragestellungen an Bedeutung. Sobald kirchliche Verwaltungsakte, Registereinträge, Personalakten, Archivunterlagen oder sonstige Verwaltungsdokumente elektronisch verarbeitet werden, handelt es sich regelmäßig um die Verarbeitung personenbezogener Daten. Das KDG erfasst nach § 2 Abs. 1 KDG die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie nichtautomatisierte Verarbeitungen, soweit die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Damit unterliegt ein erheblicher Teil kirchlicher Verwaltungspraxis unmittelbar den Vorgaben des Kirchlichen Datenschutzgesetzes. Das KDG schützt nach § 1 KDG den Einzelnen davor, durch die Verarbeitung personenbezogener Daten in seinem Persönlichkeitsrecht beeinträchtigt zu werden. Digitale Verwaltungsverfahren müssen daher zugleich datenschutzrechtlich beherrschbar bleiben.

Die allgemeinen Grundsätze kirchlicher Datenverarbeitung verdeutlichen die datenschutzrechtliche Relevanz digitaler Verwaltungsverfahren. § 6 KDG regelt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und verlangt, dass jede Verarbeitung auf eine tragfähige Rechtsgrundlage gestützt werden kann.⁸³ Für kirchliche Verwaltung kommen insbesondere eine kirchliche oder staatliche Rechtsvorschrift, eine rechtliche Verpflichtung sowie die Wahrnehmung einer Aufgabe in Betracht, die im kirchlichen Interesse liegt oder in Ausübung übertragener öffentlicher Gewalt erfolgt.⁸⁴ Die materiellen Verarbeitungsgrundsätze enthält § 7 KDG. Danach müssen personenbezogene Daten rechtmäßig und nachvollziehbar verarbeitet, für festgelegte, eindeutige und legitime Zwecke erhoben, auf das notwendige Maß beschränkt, sachlich richtig gehalten und nur so lange gespeichert werden, wie es für die jeweiligen Zwecke erforderlich ist.⁸⁵ Zudem müssen sie in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich

⁸² Nach § 33 Abs. 5 KDG sind Datenschutzverletzungen einschließlich der damit zusammenhängenden Tatsachen, Auswirkungen und Abhilfemaßnahmen zu dokumentieren. Hat die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, ist nach § 34 Abs. 1 KDG die betroffene Person zu benachrichtigen.

⁸³ Vgl. § 6 Abs. 1 KDG.

⁸⁴ Vgl. § 6 Abs. 1 lit. a, d und f KDG.

⁸⁵ Vgl. § 7 Abs. 1 lit. A-e KDG.

des Schutzes vor unbefugter Verarbeitung, Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen.⁸⁶ Für kirchliche Stellen ergibt sich daraus, dass Zugriffe, Änderungen und Übermittlungen personenbezogener Daten nachvollziehbar dokumentiert bleiben müssen. Datenschutzrechtliche Anforderungen beziehen sich damit auf den gesamten Verarbeitungsvorgang und nicht lediglich auf einzelne Datenbestände.⁸⁷

Die allgemeinen Verarbeitungsgrundsätze werden durch § 26 KDG weiter konkretisiert. Die Bestimmung verpflichtet Verantwortliche und Auftragsverarbeiter, unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen.⁸⁸ Diese Maßnahmen müssen ein dem Risiko angemessenes Schutzniveau gewährleisten; die Einhaltung der datenschutzrechtlichen Grundsätze muss zudem nachweisbar bleiben.⁸⁹ Elektronische Verwaltungsakten dürfen daher weder frei zugänglich gespeichert noch beliebig vervielfältigt werden. Ebenso muss feststellbar bleiben, wann Dokumente verändert wurden und welche Personen Zugriff auf bestimmte Informationen hatten. Gerade kirchliche Verwaltung verarbeitet häufig sensible personenbezogene Daten, etwa in Personalangelegenheiten, disziplinarischen Verfahren, der Vermögensverwaltung oder der kirchlichen Gerichtsbarkeit. Der Schutz solcher Informationen berührt daher sowohl Fragen technischer Sicherheit als auch die kirchliche Amtsverschwiegenheit und den Persönlichkeitsschutz. § 27 KDG ergänzt diese Anforderungen durch den Grundsatz datenschutzgerechter Technikgestaltung und datenschutzfreundlicher Voreinstellungen. Datenschutz muss daher bereits in die Struktur digitaler Verwaltungs- und Kommunikationssysteme integriert werden.

Datenschutzrechtliche Anforderungen reichen bis in den Bereich kirchlicher Archivführung hinein. Nach c. 486 § 1 CIC sind alle Dokumente, welche die geistlichen oder zeitlichen Angelegenheiten der Diözese betreffen, sorgfältig aufzubewahren. C. 486 § 3 CIC verlangt außerdem ein Inventar oder Verzeichnis der archivierten Dokumente. Der Zugang zum Archiv ist nach c. 487 CIC kontrolliert ausgestaltet; die Entfernung von Dokumenten aus dem Archiv ist nach c. 488 CIC nur unter den dort genannten Voraussetzungen zulässig. Für geheime Unterlagen sieht c. 489 § 1 CIC ein Geheimarchiv oder wenigstens einen besonders gesicherten Schrank vor.⁹⁰

Für digitale Verwaltungssysteme besitzt die Nachvollziehbarkeit der Verarbeitungsvorgänge eigenständige Bedeutung. Elektronische Verwaltungssysteme müssen so ausgestaltet sein, dass spätere Kontrollen und Überprüfungen möglich bleiben. § 76 Abs. 1 BDSG verlangt für automatisierte Verarbeitungssysteme insbesondere die Protokollierung von Erhebung,

⁸⁶ Vgl. § 7 Abs. 1 lit. f KDG.

⁸⁷ Einen staatlichen Vergleichspunkt bietet § 64 BDSG. Danach müssen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden (§ 64 Abs. 2 Satz 2 Nr. 1 BDSG). § 64 Abs. 3 BDSG konkretisiert diese Verpflichtung durch Maßnahmen wie Zugangs-, Benutzer-, Zugriffs-, Speicher- und Übertragungskontrollen (vgl. § 64 Abs. 3 Satz 1 Nr. 1-14 BDSG).

⁸⁸ Vgl. § 26 Abs. 1 KDG.

⁸⁹ Vgl. § 26 Abs. 1 KDG; § 7 Abs. 2 KDG. § 26 Abs. 1 KDG nennt insbesondere Pseudonymisierung, Anonymisierung und Verschlüsselung personenbezogener Daten, die dauerhafte Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, die Wiederherstellung von Verfügbarkeit und Zugang nach einem Zwischenfall sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Schutzmaßnahmen.

⁹⁰ Vgl. § 35 Abs. 1 Sätze 1-2 BNotO; § 9b Abs. 1 EGovG. Sowohl notarielle als auch staatliche elektronische Verwaltungsverfahren binden die Verarbeitung personenbezogener Daten an Vertraulichkeit, Zweckbindung und besondere Schutzmaßnahmen. Digitale Datenverarbeitung bleibt damit Teil eines rechtlich kontrollierten Verwaltungssystems.

Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung personenbezogener Daten. Zur rechtlichen Verlässlichkeit gehört daher die Möglichkeit, die Verarbeitungsgeschichte administrativer Informationen später nachvollziehen zu können. Das KDG legt zudem eine entsprechende Nachweisstruktur an. Nach § 7 Abs. 2 KDG ist der Verantwortliche für die Einhaltung der Verarbeitungsgrundsätze verantwortlich und muss dies nachweisen können. § 31 Abs. 1 KDG verpflichtet jeden Verantwortlichen zur Führung eines Verzeichnisses „zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.“ Dieses Verzeichnis hat insbesondere Angaben zu Zwecken der Verarbeitung, Kategorien betroffener Personen und personenbezogener Daten, Empfängern, Löschfristen sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zu enthalten. Die kirchliche Verwaltung muss daher gewährleisten, dass Zugriffe, Änderungen und Übermittlungen personenbezogener Daten nachvollziehbar dokumentiert bleiben.

Zusätzliche Fragen entstehen bei der Archivierung personenbezogener Daten. § 6 Abs. 3 KDG stellt klar, dass eine Verarbeitung für im kirchlichen Interesse liegende Archivzwecke nicht als Verarbeitung für einen anderen Zweck gilt, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen. § 11 Abs. 2 lit. j KDG erlaubt unter bestimmten Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten für im kirchlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke.⁹¹ Diese Möglichkeit bleibt jedoch an angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person gebunden.⁹² Elektronische Archivsysteme müssen deshalb nicht nur eine langfristige Speicherung gewährleisten, sondern zugleich differenzierte Zugriffsbeschränkungen und Schutzmechanismen gegen unbefugte Nutzung vorsehen.⁹³ Diese Spannung zeigt sich vor allem bei den Rechten betroffener Personen. Nach § 18 Abs. 2 Satz 1 KDG besteht das Recht auf Berichtigung nicht, wenn personenbezogene Daten zu Archivzwecken im kirchlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der Daten, ist ihr jedoch die Möglichkeit einer Gegendarstellung einzuräumen; das zuständige Archiv hat diese Gegendarstellung den Unterlagen hinzuzufügen.⁹⁴

Datenschutzrechtliche Fragen stellen sich nicht nur bei Speicherung und Archivierung, sondern ebenso bei der elektronischen Übermittlung von Verwaltungsakten und Verwaltungsdokumenten. Werden personenbezogene Daten elektronisch versandt, muss

⁹¹ Siehe auch § 11 Abs. 2 lit. k-l KDG: „k) die Verarbeitung ist für Zwecke der institutionellen Aufarbeitung von sexualisierter Gewalt und anderen Formen des Missbrauchs auf der Grundlage kirchlichen Rechts erforderlich und die Interessen der betroffenen Person (§ 4 Nr. 1) sind durch angemessene Maßnahmen gewahrt oder l) die Verarbeitung ist aus Gründen eines erheblichen kirchlichen oder öffentlichen Interesses zwingend erforderlich.“

⁹² Vgl. § 11 Abs. 4 KDG.

⁹³ Vgl. § 5 Abs. 5 BArchG. Der Wortlaut erlaubt die Verarbeitung personenbezogener Informationen zu Archivzwecken, bindet diese jedoch an den Schutz schutzwürdiger Belange betroffener Personen. Archivierung und Datenschutz werden damit als miteinander zu vereinbarende Rechtsgüter verstanden.

⁹⁴ Vgl. § 18 Abs. 2 Sätze 2-3 KDG. Das KDG berücksichtigt bei Archivgut sowohl die Interessen betroffener Personen als auch die Integrität archivierter Bestände. Mehrere Betroffenenrechte werden deshalb zugunsten im kirchlichen Interesse liegender Archivzwecke eingeschränkt (vgl. §§ 17 Abs. 5, 19 Abs. 3 lit. d, 20 Abs. 4, 22 Abs. 5 KDG). § 18 Abs. 3 KDG legt fest: „Dem Recht auf Berichtigung ist nur in Form von ergänzenden Eintragungen zu entsprechen, wenn ansonsten der Erhalt oder die Gewährleistung der Nachvollziehbarkeit von Amtshandlungen sowie von Urkunden und vergleichbaren Dokumenten gefährdet würde. Hierzu gehören insbesondere die durch kirchliche Rechtsvorschriften vorgesehenen Eintragungen in die Kirchenbücher (insbesondere Taufen, Trauungen, Todesfälle) sowie Dekrete, Beschlüsse von Gremien der Diözesen und Kirchengemeinden und sonstige Urkunden.“

verhindert werden, dass unbefugte Dritte vom Inhalt Kenntnis erhalten oder Dokumente unbemerkt verändert werden können. Das KDG regelte noch bis zum 1. März 2026 die Offenlegung personenbezogener Daten gegenüber kirchlichen und öffentlichen Stellen in § 9 KDG und gegenüber nichtkirchlichen und nichtöffentlichen Stellen in § 10 KDG. In beiden Fällen setzte die Übermittlung Erforderlichkeit, Zweckbindung und die Verantwortung der offenlegenden Stelle voraus.⁹⁵ Der Empfänger durfte die Daten grundsätzlich nur zu dem Zweck verarbeiten, zu dem sie ihm offengelegt wurden.⁹⁶ § 9 KDG und § 10 KDG sind mit dem Gesetz zur Änderung des KDG vom 5. Februar 2026 aufgehoben worden. Das KDG enthält nun ausschließlich mit § 29 KDG eine eigene Regelung zur Auftragsverarbeitung. Danach darf ein Verantwortlicher nur mit Auftragsverarbeitern zusammenarbeiten, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen im Einklang mit dem KDG durchgeführt werden.⁹⁷ Der zugrunde liegende Vertrag oder ein anderes Rechtsinstrument hat insbesondere Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Pflichten und Rechte des Verantwortlichen festzulegen.⁹⁸

Die digitale Zwischenspeicherung verlangt klare rechtliche Grenzen. Nach § 9b Abs. 3 EGovG ist durch technische und organisatorische Maßnahmen sicherzustellen, dass unzuständige Behörden keinen Zugriff auf zwischengespeicherte Verfahrensdaten erhalten; außerdem sind solche Daten nach Wegfall der Erforderlichkeit oder nach Ablauf der gesetzlichen Fristen zu löschen. Elektronische Verwaltung setzt damit nicht nur sichere Übermittlung, sondern kontrollierte Speicherung, begrenzte Zugänglichkeit und geregelte Löschung voraus. Entsprechendes ergibt sich kirchlich aus § 7 Abs. 1 lit. e KDG. Danach dürfen personenbezogene Daten nur so lange in identifizierbarer Form gespeichert werden, wie es für die Zwecke der Verarbeitung erforderlich ist. Archivrechtlich ist dabei zu beachten, dass Löschung und Archivierung nicht schematisch gleichgesetzt werden dürfen. § 15 Abs. 2 BArchG begrenzt den Rückgriff öffentlicher Stellen auf archivierte Unterlagen mit personenbezogenen Informationen, die vor ihrer Vernichtung oder Löschung an das Bundesarchiv abgegeben worden sind. Nach der Archivierung besteht Zugang nur noch nach Maßgabe archivrechtlicher Nutzungsvorschriften und nicht mehr ohne Weiteres zu den ursprünglichen Verwaltungszwecken. Archivierung verändert damit den rechtlichen Zugriffszusammenhang. Für kirchliche Archive ist dieser Gedanke bedeutsam, weil digitale Verwaltungsunterlagen langfristig verfügbar bleiben können und deshalb klare Grenzen zwischen laufender Verwaltung und archivarischer Nutzung erforderlich sind.⁹⁹

Zur datenschutzrechtlichen Kontrolle digitaler Verwaltungssysteme sieht das KDG zudem institutionelle Sicherungsmechanismen vor. Nach § 36 KDG haben kirchliche Stellen unter den

⁹⁵ Vgl. § 9 Abs. 1 und 4 KDG 2018; § 10 Abs. 1 und 4 KDG 2018.

⁹⁶ Vgl. § 9 Abs. 4 KDG 2018; § 10 Abs. 4 KDG 2018; § 5 Abs. 5 Satz 3 VwZG; §§ 18, 26a BNotO. Elektronische Kommunikation und Datenverarbeitung bleiben an Vertraulichkeit, Zweckbindung und kontrollierte Zugriffsberechtigungen gebunden, auch wenn externe Dienstleister eingebunden werden.

⁹⁷ Vgl. § 29 Abs. 1 KDG.

⁹⁸ Vgl. § 29 Abs. 3, Abs. 4 lit. a-b KDG. Die Einbindung externer Dienstleister entbindet nicht von den Anforderungen an Weisungsgebundenheit und Vertraulichkeit. Dies gilt zugleich für Prüfungs- und Wartungstätigkeiten, bei denen ein Zugriff auf personenbezogene Daten möglich ist.

⁹⁹ Vgl. § 35 Abs. 6 BNotO. Nach Ablauf der Aufbewahrungsfrist sind bestimmte notarielle Unterlagen dem zuständigen öffentlichen Archiv anzubieten; im Übrigen sind elektronisch geführte Akten und Verzeichnisse zu löschen. Damit wird ausdrücklich zwischen weiterer Verwahrung, archivischer Übernahme und Löschung unterschieden.

dort genannten Voraussetzungen einen betrieblichen Datenschutzbeauftragten zu benennen. Dieser ist nach § 37 KDG frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden und bei der Wahrnehmung seiner Aufgaben zu unterstützen.¹⁰⁰

Die genannten staatlichen Vorschriften gelten nicht für kirchliche Verwaltungsverfahren. Sie verdeutlichen jedoch die allgemeinen rechtlichen Anforderungen moderner digitaler Verwaltung. Elektronische Verwaltungsverfahren sind nur dann rechtlich tragfähig, wenn Vertraulichkeit, Zugriffsschutz, Nachvollziehbarkeit, sichere Übermittlung, geregelte Löschung und archivrechtlich kontrollierte Weiternutzung zuverlässig gewährleistet werden. KDG, BDSG, EGovG, BArchG und BNotO gehen übereinstimmend davon aus, dass digitale Informationsverarbeitung kontrollierte technische und organisatorische Sicherungsstrukturen voraussetzt. Für kirchliche Verwaltungssysteme folgt daraus, dass digitale Verfahren nicht allein unter dem Gesichtspunkt von Authentizität, Integrität und Beweisbarkeit betrachtet werden dürfen. Gleichrangig bleibt der Schutz personenbezogener Daten innerhalb kirchlicher Verwaltungsstrukturen. Elektronische Verwaltungssysteme müssen daher sowohl den Anforderungen des kanonischen Verwaltungsrechts als auch den datenschutzrechtlichen Vorgaben des KDG und den allgemeinen informations-, archiv- und notarrechtlichen Sicherungsstandards moderner digitaler Verwaltung entsprechen.

9 Bundes- und bayerischer Rechtsrahmen

Neben dem kanonischen Recht und dem kirchlichen Datenschutzrecht besitzt das staatliche Recht erhebliche Bedeutung für die praktische Ausgestaltung digitaler Verwaltungsverfahren. Dies gilt insbesondere dort, wo kirchliche Einrichtungen organisatorisch vergleichbare Verwaltungsstrukturen verwenden oder im staatlichen Rechtsverkehr handeln. Im bayerischen Kontext sind hierbei vor allem das Bayerische Archivgesetz sowie die Regelungen über elektronische Verwaltung von Bedeutung. Hinzu tritt das E-Government-Gesetz des Bundes als Ausdruck eines allgemeinen Strukturwandels administrativer Verfahren. Für notarielle Dokumentations- und Sicherungsfunktionen sind darüber hinaus die Bundesnotarordnung sowie die Verordnung über die Führung notarieller Akten und Verzeichnisse von besonderem Interesse, weil sie organisatorische und technische Anforderungen an elektronische Aktenführung, Dokumentensicherung und Langzeitarchivierung formulieren.¹⁰¹ Für kirchliche Stellen ist dieser staatliche Rechtsrahmen stets zusammen mit den Vorgaben des KDG zu berücksichtigen.¹⁰²

100 Vgl. §§ 37-38, 42-48 KDG. Das KDG sichert die Einhaltung datenschutzrechtlicher Anforderungen durch Datenschutzbeauftragte, Datenschutzaufsicht sowie besondere Melde- und Dokumentationspflichten bei Datenschutzverletzungen (vgl. §§ 33-34 KDG).

101 Vgl. § 1 BNotO; §§ 3-4 NotAktVV. Siehe auch Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz - BayDiG) vom 22. Juli 2022 (GVBl. S. 374, BayRS 206-1-D), das zuletzt durch § 45 des Gesetzes vom 26. März 2026 (GVBl. S. 75) geändert worden ist; hier: Art. 4 Abs. 1; Art. 5 Abs. 1.

102 Vgl. §§ 2, 6, 7, 26 KDG; Art. 16 Satz 1 BayDiG; Art. 12 Abs. 1 BayDiG; siehe auch Bayerisches Datenschutzgesetz (BayDSG) vom 15. Mai 2018 (GVBl. S. 230, BayRS 204-1-I), das zuletzt durch § 2 des Gesetzes vom 25. Juli 2025 (GVBl. S. 254) geändert worden ist; hier: Art. 4 Abs. 1, Art. 5 Abs. 1 und 3, Art. 11. Jede Behörde ist verpflichtet, einen Zugang für die Übermittlung digitaler sowie schriftformersetzender Dokumente zu eröffnen. Zugleich wird ein Anspruch auf digitale Kommunikation mit den Behörden normiert. Das BayDSG ergänzt diesen Rahmen durch Anforderungen an Rechtmäßigkeit, zweckgebundene Übermittlung, Prüfung und Wartung automatisierter Verfahren sowie Datengeheimnis.

Das Bayerische Archivgesetz enthält grundlegende Vorschriften über die dauerhafte Sicherung archivwürdiger Unterlagen öffentlicher Stellen. Es richtet sich an staatliche und kommunale Behörden. Für die kirchliche Verwaltung kann es daher lediglich als Vergleichsmaßstab dafür herangezogen werden, wie digitale Verwaltungsdokumente langfristig gesichert und geordnet verwahrt werden können. Diese Anforderungen entsprechen funktional den kirchenrechtlichen Vorgaben über die Sicherung kirchlicher Archive.¹⁰³ § 26 Abs. 1 KDG konkretisiert dies durch die Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, insbesondere zur Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit und regelmäßiger Überprüfung der Schutzmaßnahmen.¹⁰⁴ Für den notariellen Bereich finden sich entsprechende Konkretisierungen in der NotAktVV.¹⁰⁵ Für die elektronische Verwaltungspraxis besitzt daneben das E-Government-Gesetz besondere Bedeutung. Es schafft den rechtlichen Rahmen für elektronische Kommunikation, elektronische Aktenführung, digitale Nachweise, Verwaltungsportale und elektronische Verfahrensabwicklung.¹⁰⁶ Für kirchliche Verfahren ist dies nicht verbindlich. Für die vorliegende Fragestellung ist besonders bedeutsam, dass Digitalisierung im staatlichen Recht nicht auf die elektronische Übermittlung einzelner Dokumente reduziert wird. Vielmehr wird der gesamte Verwaltungsprozess in den Blick genommen.¹⁰⁷ Das Verwaltungsverfahrensgesetz verdeutlicht diesen Ansatz. § 3a Abs. 1 VwVfG bestimmt: „Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.“ Elektronische Kommunikation ist damit grundsätzlich anerkannt. Zugleich verlangt § 3a Abs. 2 Satz 1 VwVfG für gesetzlich angeordnete Schriftform grundsätzlich die qualifizierte elektronische Signatur. § 3a Abs. 3 VwVfG verlangt zudem dauerhafte Überprüfbarkeit bei elektronischen Nachweisen.¹⁰⁸

103 Vgl. c. 486 §§ 1-3 CIC; cc. 487-490 CIC; § 7 Abs. 1 lit. f KDG; siehe auch Bayerisches Archivgesetz (BayArchivG) vom 22. Dezember 1989 (GVBl. S. 710, BayRS 2241-1-WK), das zuletzt durch Gesetz vom 23. Dezember 2025 (GVBl. S. 652) geändert worden ist; hier: Art. 2 Abs. 1-3; Art. 9 Abs. 1 Satz 1; ferner Art. 26 BayDSG. Die kirchlichen Archivnormen verbinden geordnete Verwahrung mit Zugangskontrolle und besonderem Schutz sensibler Unterlagen. Das BayArchivG erfasst ausdrücklich zudem Dateien und sonstige Datenträger und versteht Archivierung als dauerhafte Verwahrung, Sicherung, Erhaltung, Nutzbarmachung und Lesbarerhaltung des Archivguts. Das BayDSG bestätigt ergänzend die datenschutzrechtliche Sonderstellung öffentlicher Archivzwecke.

104 Vgl. § 26 Abs. 1 lit. b-d KDG; Art. 19 Abs. 3 BayDiG; Art. 31 Abs. 2 BayDiG.

105 Vgl. §§ 3 Abs. 1, 4 Abs. 1 NotAktVV; Art. 2 Abs. 1 Satz 2 und Abs. 3 BayArchivG. Elektronische Dokumente müssen dauerhaft lesbar, fälschungssicher und in geeigneten Dateiformaten geführt werden.

106 Vgl. § 6 Abs. 1 EGovG; Art. 4 Abs. 5 Satz 2 BayArchivG. Während das EGovG die elektronische Abwicklung von Verwaltungsleistungen voraussetzt, verlangt das BayArchivG bereits bei Einführung oder wesentlicher Änderung informationstechnischer Systeme die Berücksichtigung späterer Archivierungsanforderungen.

107 Vgl. Art. 33 Abs. 1 BayDiG. Staatliche Behörden sollen ihre Akten digital führen. Dabei sind die Grundsätze ordnungsgemäßer Aktenführung zu wahren sowie Schutzmaßnahmen gegen Informationsverlust, unberechtigten Zugriff und Veränderungen sicherzustellen. Das KDG folgt dieser strukturellen Sicht, weil es nicht nur einzelne Daten schützt, sondern den gesamten Verarbeitungsvorgang von Erhebung, Speicherung, Veränderung, Offenlegung, Einschränkung, Löschung und Vernichtung erfasst; vgl. § 4 Nr. 3 KDG. Vgl. ferner Art. 3, Art. 4 Abs. 1, Art. 6 Abs. 4 und Art. 7 BayDSG sowie Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) in der in der Bayerischen Rechtssammlung (BayRS 2010-1-I) veröffentlichten bereinigten Fassung, das zuletzt durch § 1 des Gesetzes vom 9. Dezember 2024 (GVBl. S. 570) und durch § 1 des Gesetzes vom 23. Dezember 2024 (GVBl. S. 599) geändert worden ist; hier: Art. 3a Abs. 1-3. Die Vorschrift regelt die elektronische Kommunikation mit Behörden, die Ersetzung der Schriftform durch qualifizierte elektronische Signaturen sowie weitere sichere elektronische Identifizierungs- und Übermittlungsverfahren.

108 Elektronische Kommunikation wird damit nur unter Bedingungen anerkannt, welche Authentizität, Integrität und Nachvollziehbarkeit sichern. Gerade hierin liegt die strukturelle Parallele zum kirchlichen Verwaltungsrecht und zu § 26 KDG, der elektronische Verarbeitungssysteme an Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit und regelmäßige Überprüfung der Schutzmaßnahmen bindet (vgl. § 26 Abs. 1 lit. b-d KDG). Siehe auch Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz (BayVwZVG) in der in der Bayerischen Rechtssammlung (BayRS 2010-2-I) veröffentlichten bereinigten Fassung, das zuletzt durch § 2 des Gesetzes vom 23. Dezember 2024 (GVBl. S. 599) geändert worden ist; hier Art. 2 Abs. 1, Art. 5 Abs. 5 Satz 1-2 und Art. 5 Abs. 7 Satz 5. Danach erfasst die Zustellung auch elektronische Dokumente; elektronische Zustellung setzt einen eröffneten Zugang voraus, verlangt qualifizierte elektronische Signatur oder qualifiziertes elektronisches Siegel sowie Schutz gegen unbefugte

Das Verwaltungszustellungsgesetz ist in diesem Zusammenhang aufschlussreich hinsichtlich der elektronischen Mitteilung. § 5 Abs. 5 Satz 3 VwZG verlangt, dass elektronische Dokumente mit einer qualifizierten elektronischen Signatur versehen und gegen unbefugte Kenntnisnahme geschützt werden. Darüber hinaus ist nach § 5 Abs. 7 Satz 5 VwZG in den Akten zu vermerken, zu welchem Zeitpunkt und an welchen Zugang das Dokument versandt wurde. Elektronische Kommunikation wird damit rechtlich nur unter der Voraussetzung kontrollierter Dokumentation und nachweisbarer Übermittlung anerkannt. Für das kirchliche Verwaltungsrecht ist derselbe Gedanke bei der rechtmäßigen und nachweisbaren Mitteilung eines Verwaltungsaktes maßgeblich.¹⁰⁹ Die NotAktVV konkretisiert diese institutionelle Sicherungsfunktion durch detaillierte Vorgaben zur elektronischen Aktenführung.¹¹⁰ Gerade hierin liegt für kirchliche Stellen ein wesentlicher Gesichtspunkt. Die rechtlichen Anforderungen betreffen nicht nur das einzelne Dokument, sondern die Organisation des gesamten Informationsbestandes. Für kirchliche Stellen stellt sich dieselbe Frage.¹¹¹

Der staatliche Rechtsrahmen betrifft jedoch nicht nur Kommunikation und Zustellung, sondern die Organisation elektronischer Verwaltungsabläufe. § 9 Abs. 1 EGovG verlangt, dass Verwaltungsabläufe, die erstmals zu wesentlichen Teilen elektronisch unterstützt werden, vor Einführung der informationstechnischen Systeme dokumentiert, analysiert und optimiert werden sollen. Für kirchliche Verwaltungen enthält dies einen wichtigen funktionalen Hinweis. Digitalisierung darf nicht auf die nachträgliche elektronische Abbildung bestehender Papierabläufe reduziert werden. Vielmehr müssen Zuständigkeiten, Verfahrensschritte, Zugriffsrechte und Dokumentationspflichten vor der technischen Umsetzung rechtlich geordnet werden.¹¹² Ein weiterer Gesichtspunkt betrifft die organisatorische Dokumentation digitaler Verarbeitungsvorgänge. § 76 Abs. 1 BDSG verlangt für automatisierte Verarbeitungssysteme insbesondere die Protokollierung von Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung personenbezogener Daten. Fehlt eine

Kenntnisnahme und einen Aktenvermerk über Zeitpunkt und Zugang der Übermittlung. Vgl. ferner Art. 33 Abs. 3 BayDiG. Ergänzend hierzu bestimmt Art. 3a Abs. 1-3 BayVwVfG die allgemeinen Voraussetzungen elektronischer Kommunikation mit Behörden und konkretisiert die Anforderungen an die rechtssichere elektronische Übermittlung sowie die Ersetzung gesetzlicher Schriftformerfordernisse.

109 So zumindest im mittlerweile aufgehobenen § 9 KDG 2018. Einen funktionalen Vergleichspunkt bietet zudem § 1 BNotO, wonach Notare als unabhängige Träger eines öffentlichen Amtes bestellt werden. Die Mitwirkung des Kanzlers oder eines Notars nach c. 474 CIC dient der Authentizität, Dokumentation und rechtlichen Verlässlichkeit kirchlicher Verwaltungsvorgänge.

110 Nach § 5 Abs. 1 NotAktVV sind Systeme zum Umgang mit elektronischen Aufzeichnungen gegen unbefugten Zugang zu schützen. § 5 Abs. 2 NotAktVV verlangt zusätzliche Sicherungen gegen Verlust, Veränderung und unzureichende Verfügbarkeit. Vergleichbar verlangt Art. 9 Abs. 1 Satz 1 BayArchivG die dauerhafte Aufbewahrung, Erhaltung und Benutzbarkeit des Archivguts sowie dessen Schutz vor unbefugter Verarbeitung. Ebenso bestimmt Art. 33 Abs. 1 Satz 3 BayDiG, dass digital geführte Akten vor Informationsverlust sowie unberechtigten Zugriffen und Veränderungen zu schützen sind. Ergänzend regelt Art. 32 Abs. 2 BayDSG für automatisierte Verarbeitung. Siehe § 6 NotAktVV sowie Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Amtsblatt der Europäischen Union, L 119, 1); hier: Art. 32.

111 Wie bereits dargelegt müssen nach § 26 Abs. 1 KDG technische und organisatorische Maßnahmen gewährleisten, dass Informationen verfügbar bleiben und Schutzmechanismen regelmäßig überprüft werden.

112 Vgl. § 31 Abs. 1 KDG. Die §§ 7-20 NotAktVV konkretisieren die elektronische Registerführung durch Anforderungen an Dokumentation, Änderungsnachweise, Export und Signierung der Verzeichnisdaten. Insbesondere verlangen §§ 19 und 20 NotAktVV die qualifizierte Signierung bestimmter Verzeichnisdaten sowie die persönliche Bestätigung wesentlicher Änderungen durch den Notar. Elektronische Registerführung wird damit an Authentizität, Verantwortlichkeit und Nachvollziehbarkeit gebunden. Vergleichbar sieht Art. 24 Abs. 3 BayDiG für digitale Verwaltungsverfahren umfassende Protokollierungspflichten vor.

nachvollziehbare Dokumentation der Verarbeitungsschritte, wird eine spätere rechtliche Überprüfung administrativer Entscheidungen erheblich erschwert.¹¹³

Eigene Anforderungen stellt schließlich die langfristige elektronische Archivierung. Die §§ 34-39 NotAktVV regeln die elektronische Urkundensammlung einschließlich Einstellung, Speicherung, Löschung und Langzeitarchivierung elektronischer Dokumente. § 35 Abs. 4 NotAktVV verlangt ausdrücklich die Verwendung einer für die Langzeitarchivierung geeigneten Variante des PDF-Formats. § 50 Abs. 1 NotAktVV sieht für zahlreiche elektronische Unterlagen Aufbewahrungsfristen von bis zu 100 Jahren vor. Langfristige elektronische Archivierung stellt daher deutlich höhere Anforderungen als die bloße Speicherung digitaler Dokumente. Das KDG trägt dieser Spannung zwischen langfristiger Aufbewahrung und Datenschutz durch besondere Archivregelungen Rechnung. Archivzwecke im kirchlichen Interesse gelten nach § 6 Abs. 3 KDG nicht als Zweckänderung, während Löschungs-, Berichtigungs- und Einschränkungrechte für Archivgut in den §§ 18-20 KDG modifiziert werden.

10 Juristische Schlussfolgerung

Die bisherigen Überlegungen zeigen, dass die Digitalisierung kirchlicher Verwaltung nicht im Widerspruch zu den Anforderungen des kanonischen Rechts stehen muss. Es kommt daher auf die rechtliche Struktur kirchlichen Verwaltungshandelns an. Der Codex verlangt in den hier relevanten Bereichen Schriftlichkeit, Unterzeichnung, Dokumentation und Archivierung. Die einschlägigen Vorschriften legen jedoch nicht ausdrücklich fest, dass diese Anforderungen ausschließlich durch papiergebundene Dokumente erfüllt werden können. Die genannten Formanforderungen dienen nach Auffassung des Verfassers der Sicherung bestimmter juristischer Funktionen, die durch Verwaltungsakte und Verwaltungsdokumente gewährleistet werden müssen. Digitale Verfahren bleiben daher nur zulässig, wenn die hierfür erforderlichen rechtlichen Sicherungsfunktionen gewahrt werden.¹¹⁴ Dies wird deutlich in den Normen über Verwaltungsakte, notarielle Mitwirkung und kirchliche Archive. Die cc. 35-58 CIC regeln die allgemeinen Voraussetzungen kirchlicher Einzelverwaltungsakte und insbesondere der Einzeldekrete. Ergänzend sichern c. 474 CIC sowie die cc. 482-484 CIC durch die Mitwirkung des Kanzlers oder eines Notars die Authentizität und Verlässlichkeit kirchlicher Verwaltungsdokumente. Die cc. 486-491 CIC verpflichten schließlich zur geordneten und sicheren Aufbewahrung kirchlicher Archive.

Die genannten Vorschriften dienen nicht lediglich formalen Zwecken.¹¹⁵ Ihr gemeinsamer Zweck besteht vielmehr darin, Authentizität, Integrität, Nachvollziehbarkeit und dauerhafte

113 Vergleichbare Sicherungsmechanismen enthält § 61 Abs. 1 Nr. 3 und 4 NotAktVV, wonach Änderungen und Löschungen elektronischer Eintragungen nachvollziehbar bleiben müssen. Im kirchlichen Datenschutzrecht wird diese Nachvollziehbarkeit durch § 7 Abs. 2 KDG sowie durch die Verzeichnis- und Dokumentationspflichten der §§ 31 und 33 KDG abgesichert. Vergleichbar verlangen Art. 24 Abs. 3 und Art. 30 Abs. 4 BayDiG die Protokollierung und dokumentierte Nachvollziehbarkeit digitaler Verwaltungsvorgänge. Ergänzend verpflichtet Art. 7 Abs. 1 Satz 2 Nr. 2 BayDSG bei automatisierten Abrufverfahren zur Feststellbarkeit und Überprüfbarkeit der Übermittlung personenbezogener Daten; Art. 32 Abs. 2 BayDSG konkretisiert dies durch Eingabe- und Übertragungskontrollen.

114 Vgl. §§ 6, 7, 26, 27 KDG.

115 Zwar sichern einzelne Vorschriften zunächst die schriftliche Dokumentation und dauerhafte Festhaltung eines Verwaltungsvorgangs. Im Zusammenwirken mit den Vorschriften über Unterzeichnung, notarielle Mitwirkung, Mitteilung und Archivierung dienen sie jedoch darüber hinaus der Gewährleistung von Authentizität, Integrität und Nachvollziehbarkeit kirchlichen Verwaltungshandelns.

Beweisbarkeit kirchlicher Verwaltungsvorgänge sicherzustellen. Maßgeblich ist daher nicht das verwendete technische Medium als solches, sondern die zuverlässige Wahrung dieser rechtlichen Sicherungsfunktionen. Die Untersuchung hat ergeben, dass die einzelnen Vorschriften trotz ihrer unterschiedlichen Regelungsgegenstände einem gemeinsamen Anliegen folgen: Verwaltungshandeln soll dokumentiert, nachvollziehbar und dauerhaft überprüfbar bleiben. Eine gegenteilige Auffassung wäre zwar vertretbar und könnte stärker auf die historische Entstehung der Vorschriften abstellen. Nach Auffassung des Verfassers überwiegen jedoch die Argumente für eine Auslegung, die an den rechtlichen Sicherungszwecken der Normen anknüpft. Danach können digitale Technologien diese Funktionen grundsätzlich ebenso erfüllen wie traditionelle papiergebundene Verfahren. Dies gilt insbesondere für elektronische Dokumentationssysteme, digitale Archive, kontrollierte Verwaltungssysteme und gesicherte Kommunikationsplattformen. Werden Dokumente innerhalb geschützter Systeme erstellt, unveränderbar gespeichert, nachvollziehbar archiviert und rechtssicher übermittelt, können Authentizität, Integrität und Nachweisbarkeit ebenso gewährleistet werden wie bei herkömmlicher papiergebundener Verwaltung. Das KDG folgt demselben Ansatz, indem es digitale Verarbeitung nicht verbietet, sondern rechtlich an geeignete technische und organisatorische Maßnahmen bindet.¹¹⁶ Ein ähnlicher Gedanke findet sich im europäischen Vertrauensdiensterecht. Die eIDAS-Verordnung schafft keinen allgemeinen kirchlichen Formersatz und regelt nicht die kanonische Gültigkeit kirchlicher Verwaltungsakte. Sie zeigt jedoch, dass elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente und Dienste für die Zustellung elektronischer Einschreiben gerade dort rechtlich anerkannt werden, wo sie Zurechnung, Herkunft, Unversehrtheit, zeitliche Einordnung und Nachweisbarkeit sichern. Besonders deutlich wird dies in Art. 46 eIDAS-VO: „Einem elektronischen Dokument darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt.“ Damit bestätigt die Verordnung den Grundgedanken, dass die elektronische Form als solche kein Hindernis für die rechtliche Anerkennung eines Dokuments mit den jeweiligen rechtlichen Sicherungsfunktionen darstellt.

Die rechtliche Tragfähigkeit digitaler Verwaltungsverfahren erschöpft sich jedoch nicht in der äußeren Form elektronischer Dokumente. Moderne digitale Verwaltung setzt kontrollierte Informationsverarbeitung voraus. Gerade hierin liegt die besondere Bedeutung des kirchlichen Datenschutzrechts. Elektronische Verwaltung bedeutet nicht lediglich digitale Kommunikation, sondern eine normativ gesteuerte Verarbeitung administrativer Informationen.¹¹⁷ Aus der Perspektive öffentlicher Beurkundung gelangt die Bundesnotarordnung zu einem vergleichbaren Ergebnis. Hier werden Authentizität, Verlässlichkeit und Nachprüfbarkeit nicht durch das technische Medium selbst, sondern durch institutionell abgesicherte Verantwortungsstrukturen gewährleistet. Für kirchliche Verwaltungsverfahren gilt funktional derselbe Grundsatz.

¹¹⁶ Vgl. §§ 26-27 KDG.

¹¹⁷ Das Bundesdatenschutzgesetz bestätigt diese Anforderungen aus staatlicher Perspektive. Die §§ 64 und 76 BDSG verbinden digitale Datenverarbeitung mit technischen Sicherungsmaßnahmen und Protokollierungspflichten. Das E-Government-Gesetz geht davon aus, dass rechtssichere Digitalisierung elektronische Aktenführung, sichere Übermittlungswege und dauerhaft nachvollziehbare Verwaltungsabläufe voraussetzt (vgl. § 6a Satz 1, § 9a Abs. 3 Nr. 5 und § 15 Abs. 1-2 EGovG). Für kirchliche Verwaltung folgt daraus kein unmittelbar anwendbares Modell, wohl aber ein tragfähiger funktionaler Vergleichsmaßstab.

Sowohl das notarielle Berufsrecht als auch das KDG gehen davon aus, dass die Nachvollziehbarkeit digitaler Dokumentation nicht isoliert betrachtet werden kann. Sie setzt vielmehr organisatorische und archivarische Sicherungen voraus.¹¹⁸ Langfristige Aufbewahrung setzt dabei den fortdauernden Schutz von Authentizität, Vertraulichkeit und Nachvollziehbarkeit voraus.¹¹⁹ Die digitale Verwaltung verlangt zudem institutionelle Kontrolle. Das KDG gewährleistet diese durch Datenschutzbeauftragte, Datenschutzaufsicht sowie Dokumentations- und Meldepflichten bei Datenschutzverletzungen. Digitale Verwaltung bleibt damit nicht nur technisch, sondern organisatorisch und aufsichtsrechtlich gebunden.

Dieses Ergebnis versteht sich nicht als zwingende Folge des Wortlauts der geltenden Normen. Zu klären ist, ob die in cc. 37, 51 und 474 CIC vorausgesetzte Schriftlichkeit und Unterzeichnung notwendig an papiergebundene Dokumente gebunden sind, bleibt letztlich eine Auslegungsfrage. Die vorliegende Untersuchung gelangt jedoch zu dem Ergebnis, dass die besseren Gründe für eine funktionale Interpretation der einschlägigen Formvorschriften sprechen. Sie bestreitet dabei nicht, dass der Codex Schriftlichkeit und Unterzeichnung verlangt. Sie vertritt vielmehr die Auffassung, dass diese Anforderungen nicht notwendig eine bestimmte materielle Trägerform voraussetzen, sofern die mit ihnen verfolgten rechtlichen Sicherungszwecke in funktional gleichwertiger Weise gewährleistet werden.

Für den Verfasser bestehen nach den vorstehenden Überlegungen keine zwingenden kanonischen Gründe, digitale Verfahren im kirchlichen Verwaltungsrecht grundsätzlich auszuschließen. Zwar enthält der Codex gegenwärtig keine ausdrücklichen Regelungen über elektronische Verwaltungsakte oder elektronische Verwaltungsdokumente. Ebenso finden sich keine universalkirchlichen Normen, welche die Verwendung digitaler Verwaltungsverfahren allgemein untersagen oder abschließend regeln. Diese normative Offenheit führt jedoch nicht zu einem rechtlichen Vakuum. Die einschlägigen Vorschriften über Verwaltungsakte, notarielle

118 Die Zivilprozessordnung ergänzt diese Bewertung um die beweisrechtliche Perspektive. § 371a ZPO ordnet für qualifiziert elektronisch signierte Dokumente besondere Beweiswirkungen an, die funktional an die Beweiskraft privater Urkunden anknüpfen. § 371b ZPO verdeutlicht zudem, dass auch die Übertragung öffentlicher Urkunden in elektronische Dokumente rechtlich anerkannt werden kann, wenn die bildliche und inhaltliche Übereinstimmung mit der Urschrift gesichert ist. Die eIDAS-Verordnung enthält entsprechende Sicherungsmechanismen. Art. 25 Abs. 2 eIDAS-VO ordnet für qualifizierte elektronische Signaturen die gleiche Rechtswirkung wie für handschriftliche Unterschriften an. Art. 35 Abs. 2 eIDAS-VO statuiert für qualifizierte elektronische Siegel die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe. Art. 41 Abs. 2 eIDAS-VO enthält entsprechende Vermutungen für qualifizierte elektronische Zeitstempel, Art. 43 Abs. 2 eIDAS-VO für qualifizierte Dienste der Zustellung elektronischer Einschreiben. Das Bundesarchivgesetz ergänzt diese Perspektive um Anforderungen der Langzeitarchivierung. Es versteht Unterlagen als Aufzeichnungen jeder Art unabhängig von ihrer Speicherung (vgl. § 1 Nr. 10 BArchG) und verlangt für elektronische Unterlagen Standards hinsichtlich Übermittlung, Datenformat und Löschungsnachweisen (vgl. § 5 Abs. 3 Satz 1-4 BArchG). Das KDG modifiziert zugleich Betroffenenrechte für Archivgut. Das Recht auf Berichtigung besteht bei archivischer Verarbeitung nicht, wobei eine Gegendarstellung beizufügen ist (vgl. § 18 Abs. 2 KDG). Ebenso bestehen Einschränkungen des Löschungsrechts zugunsten kirchlicher Archivzwecke (vgl. § 19 Abs. 3 lit. d KDG) sowie der Rechte auf Einschränkung der Verarbeitung und Datenübertragbarkeit (vgl. § 20 Abs. 4 KDG; § 22 Abs. 5 KDG).

119 Die eIDAS-Verordnung berücksichtigt die Langzeitbewahrung elektronischer Nachweise. Erwägungsgrund 61 betont die Sicherung der rechtlichen Gültigkeit und Validierbarkeit elektronischer Signaturen und Siegel über lange Zeiträume. Art. 34 Abs. 1 eIDAS-VO regelt qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen; Art. 40 eIDAS-VO überträgt diese Regelungen auf qualifizierte elektronische Siegel. § 15 VDG ergänzt diese Struktur, indem qualifiziert signierte, gesiegelte oder zeitgestempelte Daten rechtzeitig erneut geschützt werden müssen, bevor der Sicherheitswert bestehender Sicherungen absinkt. Art. 5 sowie Art. 12 Abs. 3 lit. c und d eIDAS-VO verdeutlichen den Zusammenhang zwischen elektronischer Identifizierung, Vertrauensdiensten und geeigneten Sicherheitsvorkehrungen. Archivrechtlich begrenzt § 14 BArchG Betroffenenrechte für Archivgut; § 15 Abs. 2 BArchG schließt die weitere Nutzung vor einer Löschung abgegebener personenbezogener Informationen durch die abgebende Stelle für deren ursprüngliche Zwecke aus. Vergleichbar beschränkt § 17 Abs. 5 KDG das Auskunftsrecht gegenüber kirchlichen Archiven. Das staatliche Verwaltungsrecht erkennt elektronische Verfahren nur unter gesicherten Voraussetzungen an (vgl. § 3a Abs. 2 Satz 1 VwVfG; § 5 Abs. 5 und 7 VwZG). Das Vertrauensdienstegesetz ergänzt diese Vorgaben auf nationaler Ebene für elektronische Signaturen, Siegel, Zeitstempel und Zustelldienste (vgl. § 1 Abs. 1 VDG).

Mitwirkung, Dokumentation, Archivierung und Datenschutz enthalten bereits heute rechtliche Maßstäbe, anhand derer digitale Verwaltungsverfahren beurteilt werden können. Die Analyse legt nahe, dass die genannten Vorschriften nicht primär bestimmte technische Trägerformen schützen, sondern rechtliche Sicherungsfunktionen. Können digitale Verfahren diese Anforderungen in funktional gleichwertiger Weise erfüllen, bestehen gegen ihren Einsatz im kirchlichen Verwaltungsrecht keine durchgreifenden rechtlichen Bedenken. Zentral ist nicht die Gegenüberstellung von Papier und Elektronik, sondern die normengerechte Beherrschbarkeit des jeweiligen Verwaltungsvorgangs. Eine zukünftige ausdrückliche Regelung durch den kirchlichen Gesetzgeber könnte zusätzliche Rechtssicherheit schaffen. Die Untersuchung legt nahe, dass digitale Kommunikations- und Informationstechnologien mit den geltenden Anforderungen des kirchlichen Verwaltungsrechts vereinbar sein können, sofern die dargestellten Sicherungsfunktionen in funktional gleichwertiger Weise gewährleistet werden.