Rundschreiben des Landeskirchenamtes an die Kirchenkreise und Verbände kirchlicher Körperschaften betreffend den kirchlichen Datenschutz: BSI-Richtlinie zur vertrauenswürdigen elektronischen Langzeitspeicherung[1]

Vom 26. Mai 2010 (Az.: 610.213/11) [aktualisiert am 31. Mai 2013]

Immer mehr Daten werden in elektronischer Form vorgehalten. Damit wird die Frage wichtig, wie die Langzeitspeicherung dieser Dokumente, Akten und Daten über die langen Aufbewahrungszeiträume professionell gesichert werden kann. Ein Problem für die Lesbarkeit und Verfügbarkeit stellen dabei die immer kürzer werdenden Innovationszyklen der Technologien von Speichermedien und Datenformaten dar. Der Zugriff auf Daten und Dokumente muss den Anforderungen des Datenschutzes und der Datensicherheit genügen, auch über lange Zeiträume und den Wechsel von IT-Systemen hinweg. Zunehmend gewinnt der Bedarf an rechtswirksamer Beweiswerterhaltung kryptographisch signierter Dokumente an Bedeutung. Dies wird an folgenden Beispielen deutlich: Elektronische Unterlagen im Gesundheitswesen, elektronische Rechnungen und Belege im täglichen Geschäftsverkehr, Kirchenbuchregister und viele Dokumente mehr verlangen nach adäquaten Lösungen im Rahmen fortschreitender Digitalisierung der Geschäfts- und Verwaltungstätigkeiten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte für den Bereich der Verwaltung des Bundes die

„Technische Richtlinie 03125: Vertrauenswürdige elektronische Langzeitspeicherung“

mit Stand vom 31. Juli 2009 in der Version 1.0 herausgegeben (jetzt Vorgängerversion). Diese Richtlinie ist zwischenzeitlich vom BSI zur

„BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente“

weiter entwickelt worden. Dabei zielt die TR-03125 nicht darauf ab, bekannte und etablierte Anforderungen und Begriffsdefinitionen zu ersetzen. Vielmehr sind zusätzlich die Anforderungen an die ordnungsgemäße Aufbewahrung für elektronisch signierte Dokumente einzuhalten. Sie werden von der TR-03125 vorausgesetzt. Die Referenz-Architektur

1 Aktualisiert am 31.05.2013 – die BSI-Richtlinie ist weiterentwickelt worden mit dem Ziel der Beweiswerterhaltung kryptographisch signierter Dokumente. Mit der Technischen Richtlinie BSI-TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume – bis zum Ende der Aufbewahrungsfristen – im Sinne eines rechtswirksamen Beweiswerterhalts vertrauenswürdig gespeichert werden können.
Redaktioneller Hinweis: Am 24. Mai 2018 ist das neu gefasste EKD-Datenschutzgesetz vom 15. November 2017 (Nr. 850) in Kraft getreten. Es wird zurzeit geprüft, ob und inwieweit eine Aktualisierung der Regelungen des Rundschreibens an das neue kirchliche Datenschutzrecht erforderlich ist.

der TR-03125 versteht sich daher nicht als Ersatz für ein Archiv-System sondern als Konzept einer Middleware, das eine mögliche Umsetzung der Anforderungen zum rechtswirksamen Beweiswerterhalt kryptographisch signierter Dokumente während des gesetzlich vorgeschriebenen Aufbewahrungszeitraums beschreibt. Die BSI-Richtlinie TR-03125 enthält im wesentlichen Erläuterungen und Empfehlungen

1. zu den Daten- und Dokumentenformaten;
2. zum Speicherformat für Archivdatenobjekte;
3. zu einer IT-Referenzarchitektur oder alternativen Architekturen;
4. zu Anforderungen an Komponenten (vorgelagerte Anwendungssysteme) und an Module (Krypto-Modul) sowie deren Abhängigkeiten.

Auf der Basis des vorliegenden Anforderungskatalogs können nun Anbieter und Produkthersteller zu dieser Richtlinie konforme Lösungsangebote entwickeln.

Die BSI-Richtlinie 03125 dient als konkrete Orientierung und Hilfestellungen auch für kirchliche Verwaltungen hinsichtlich der

- Verfügbarkeit und Lesbarkeit,
- Integrität und Authentizität,
- Datenschutz und Datensicherheit,

elektronischer Daten aller Art über lange Aufbewahrungszeiträume hinweg.

Konkret beschreibt diese Technische Richtlinie einen differenzierten Katalog von verpflichtenden (Muss), von empfohlen (Soll) und auch von optionalen (Kann) Anforderungen im Hinblick auf alle Elemente und Bereiche, in denen ein Gestaltungsbedarf besteht, um für Behörden und Institutionen wirkungsvolle, zukunftssichere und wirtschaftliche technische Szenarien für eine beweiswerterhaltende Aufbewahrung elektronisch signierter Dokumente und Daten aufzubauen.

Für die Aufbewahrung elektronischer Dokumente ist aus der Perspektive des Datenschutzes vor allem auf § 9 DSG-EKD[1] und die dazugehörige Anlage aufmerksam zu machen. Das heißt insbesondere für personenbezogenen Daten bedarf es einer angemessenen organisatorischen und technischen Sicherung durch

1. Zugriffskontrolle,
2. Weitergabekontrolle,
3. Eingabekontrolle.

Das bedeutet, dass durch organisatorische und technische Maßnahmen sicherzustellen ist, dass nicht autorisierte Zugänge und Zugriffe auf schützenswerte Daten zuverlässig verhindert werden, Informationen und Daten weder vorsätzlich noch fahrlässig unbemerkt

1 Nr. **850 Archiv-1**.

und in unzulässiger Weise manipuliert werden können, Veränderungen daran protokolliert werden und ein unwiederbringlicher Verlust schützenswerter Informationen und Daten ausgeschlossen werden kann. Der Einsatz von kryptografischen Verschlüsselungstechniken sowie die strikte logische oder auch physikalische Trennung schützenswerter Daten und Informationen sind hierfür geeignete Instrumente.

Ein erhöhter Schutzbedarf ergibt sich überall dort, wo personenbezogene Daten beispielsweise der ärztlichen Schweigepflicht oder Amts-, Berufs- und Geschäftsgeheimnissen unterliegen.

Aus datenschutzrechtlicher Sicht ist zusätzlich § 16 DSG-EKD[1] zu beachten, wonach personenbezogene Daten zu löschen oder zu sperren sind, wenn ihre Kenntnis für die verantwortliche kirchliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Dies bedeutet für elektronische Archivierungssysteme, dass nach Ablauf der vorgeschriebenen Mindestaufbewahrungsfristen die Datenobjekte in der kirchlichen Verwaltung dann aus dem Langzeitspeicher gelöscht werden sollen, wenn diese zuvor dem zuständigen Archiv angeboten und von diesem übernommen wurden bzw. wenn das Archiv die Ermächtigung zum Löschen erteilt hat.

Wir empfehlen aus datenschutzrechtlicher Sicht insbesondere beim Einsatz von Software zur Langzeitspeicherung die Vorgaben und Empfehlungen der „BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente“ „zu beachten. Die Richtlinie ist (ebenso wie die Vorgängerversion „BSI-Richtlinie BSI TR-031125 zur vertrauenswürdigen elektronischen Langzeitspeicherung“) über das Internet über den Link https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html in der jeweils aktuellen Fassung abrufbar.

Für die Aufbewahrung von Akten der öffentlichen Verwaltung, insbesondere für die Einführung der elektronischen Akte ist bereits früher über den IT-Beauftragten der Bundesregierung für Informationstechnik ein Konzept für Dokumenten-Management und elektronische Archivierung, das **DOMEA-Konzept** entwickelt worden, deren Inhalte teilweise durch die BSI-Richtlinie[2] konkretisiert bzw. modifiziert werden. Seit November 2005 liegt DOMEA in der Version 2.1 vor. Den Hersteller von Dokumenten-Management- und Archivierungssystemen wurde über DOMEA die Möglichkeit der Zertifizierung ihrer DVProdukte angeboten; dies ist in den vergangenen Jahren von verschiedenen Firmen, die als Kunden die öffentliche Verwaltung im Blick haben, wahrgenommen worden. Die Bundesregierung hat im Regierungsprogramm „Vernetzte und transparente Verwaltung“ beschlossen, ein neues Konzept zu erarbeiten, das den organisatorischen Rahmen für die elektronische Verwaltungsarbeit definiert (**Organisationskonzept Elektronische Verwaltungsarbeit**). Das neue "Organisationskonzept elektronische Verwaltungsarbeit" löst das bisherige DOMEA-Konzept ab. Das Zertifizierungsverfahren wird nicht fortgesetzt.

---

1 Nr. **850 Archiv-1**.

2 siehe die Ausführungen zum DOMEA-Konzept in der BSI-Richtlinie u. a. unter 6.2

Das "Organisationskonzept elektronische Verwaltungsarbeit" unterstützt Behörden dabei, aus dem großen Angebot die für sie passenden Verfahren auszuwählen und erfolgreich in die Praxis umzusetzen. Mit der Informations- und Kommunikationstechnologie soll die Tätigkeit der öffentlichen Verwaltung effektiver und effizienter gestaltet werden. So ist die elektronische Kommunikation längst selbstverständlich. Schriftgut kann elektronisch verwaltet, Prozesse können elektronisch abgewickelt werden. Hinzu kommen neue Entwicklungen, wie Bürgerportale, soziale Netzwerke oder Wikis. Elektronische Verwaltungsarbeit im Sinne dieses Konzepts umfasst:

- elektronische Schriftgutverwaltung (E-Akte) einschließlich der elektronischen Langzeitspeicherung und Aussonderung sowie
- elektronische Prozessunterstützung durch:
    - elektronische Vorgangsbearbeitung,
    - elektronische Zusammenarbeit und
    - Fachverfahren.

Das Organisationskonzept ist nach dem Baukastensystem aufgebaut. Die folgenden Bausteine sind verfügbar:

- Grundlagen und Bedarfsanalyse,
- E-Akte,
- E-Vorgangsbearbeitung,
- E-Zusammenarbeit,
- Projektleitfaden,
- Glossar.

Weitere Bausteine befinden sich in Arbeit bzw. in Planung:

- E-Langzeitspeicherung (in Arbeit)
- E-Langzeitspeicherung (in Arbeit)
- E-Poststelle und Signatur (in Arbeit)
- Scan-Prozess (in Arbeit)
- Datenschutz, Personaldaten und VS (in Planung)
- E-Fachverfahren (in Planung)

Während einer Übergangsphase können Information zum bisherigen DOMEA-Organisationskonzept 2.1, die Erweiterungsmodule, den Anforderungskatalog und weitere Dokumente unter http://www.verwaltung-innovativ.de/cln_319/nn_684536/sid_0FFA58BA226D9BD9B9F94469B73EE29C/DE/Organisation/domea__konzept/domea__konzept__inhalt.html?__nnn=true aufgerufen werden.

Soweit bei Ihnen Überlegungen zur Langzeitspeicherung elektronischer Dokumente bzw. die Anschaffung entsprechender Software anstehen, bitten wir die Vorgaben der BSI-Richtlinie TR-03125 zu beachten und mit den Software-Herstellern von Dokumenten-Mangement- und Archivierungssystemen abzuklären, inwieweit die DV-Produkte den Anforderungen der BSI-Richtlinie entsprechen und/oder ob eine Zertifizierung nach dem alten DOMEA-Konzept vorliegt bzw. die Vorgaben und Empfehlungen des neuen „Organisationskonzepts elektronische Verwaltungsarbeit" unterstützt werden.

Zudem sind die Vorgaben aus dem Archivgesetz zu beachten bzw. sinngemäß anzuwenden. Bereits bei der Einführung entsprechender Programme ist daher das Landeskirchliche Archiv zur Abstimmung der archivfachlichen Belange zu beteiligen. Aus archivarischer Sicht sind einheitliche DMS-Lösungen wünschenswert.

Bisher ist im Muster-IT-Sicherheitskonzept kein entsprechender Baustein zur Langzeitarchivierung vorhanden. Sobald ein entsprechender Baustein im Muster-IT-Sicherheitskonzept implementiert wird, sind die dort enthaltenen Vorgaben für die kirchlichen Körperschaften der Evangelischen Kirche von Westfalen vorrangig zu berücksichtigen.

Wir bitten das Rundschreiben insbesondere an die EDV-Leitungen, an die mit der IT-Sicherheit beauftragten Personen sowie an die örtlichen Beauftragten und Betriebsbeauftragten für den Datenschutz weiterzuleiten.

Bitte informieren Sie gegebenenfalls auch die Kirchengemeinden, die kirchlichen Verbände sowie die diakonischen Einrichtungen, soweit dort Überlegungen oder Entscheidungen zur Einführung von Archivierungssoftware o. ä. anstehen.