Durchführungsbestimmungen zur Datenablage in Clouddiensten (DB-Ablage-Cloud - DB Cloud)

Vom 10. Dezember 2024 (GVBl. 2025, Nr. 25, S. 72)

Der Evangelische Oberkirchenrat erlässt nach § 2 des Kirchlichen Gesetzes zur Ausführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (AusG-DSG-EKD) vom 25. April 1994 (GVBl. S. 107), geändert am 23. Oktober 2013 (GVBl. S. 295) in Verbindung mit § 54 Abs. 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 15. November 2017 (ABl. EKD S. 353), zuletzt geändert am 9. November 2022 (ABl. EKD S. 156) folgende Durchführungsbestimmungen:

§ 1
Geltungsbereich, Begriffsbestimmungen

(1) Diese Durchführungsbestimmungen finden Anwendung auf alle haupt- und ehrenamtlich Mitarbeitenden (Nutzende) der Evangelischen Landeskirche in Baden, der Kirchenbezirke und Kirchengemeinden sowie der Zweckverbände (Artikel 107 GO).

(2) Diese Durchführungsbestimmungen beziehen sich ausschließlich auf die Nutzung der Clouddienste, die von der IT-Abteilung des Evangelischen Oberkirchenrats den Nutzenden zur Verfügung gestellt werden.

(3) Verantwortliche Stelle (§ 4 Nr. 9 DSG-EKD) im Sinne dieser Durchführungsbestimmungen sind die Evangelische Landeskirche in Baden, Kirchenbezirke und Kirchengemeinden sowie Zweckverbände nach Artikel 107 GO ebenso wie besondere Gemeindeformen nach Artikel 30 GO, soweit die genannten Rechtsträger über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

§ 2
Einordnung in Schutzklassen

(1) [1]Der Schutzbedarf personenbezogener Daten ist von der verantwortlichen Stelle (§ 4 Nr. 9 DSG-EKD) anhand einer Daten- bzw. Risikoanalyse festzustellen. [2]Nach erfolgter Analyse werden die personenbezogenen Daten einer der in § 3 genannten vier Datenschutzklassen zugeordnet.

(2) [1]Für eine Analyse der möglichen Risiken für die Rechte und Freiheiten natürlicher Personen, die mit der Verarbeitung personenbezogener Daten verbunden sind, sind objektive Kriterien zu entwickeln und anzuwenden. [2]Hierzu zählen insbesondere die Eintrittswahrscheinlichkeit und die Schwere eines Schadens für die betroffene Person. [3]Zu berücksichtigen sind auch Risiken, die durch - auch unbeabsichtigte oder

unrechtmäßige - Vernichtung, durch Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten entstehen.

(3) [1]Bei der Einordnung personenbezogener Daten in eine Datenschutzklasse sind auch der Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Interesse an einer missbräuchlichen Verwendung der Daten zu berücksichtigen. [2]Der örtlich Beauftragte für den Datenschutz soll angehört werden.

§ 3
Einstufung des Schutzbedarfs

(1) Der Schutzbedarf der personenbezogenen Daten wird entsprechend der folgenden Gewichtungen und Beschreibungen festgelegt:

1. Geringer Schutzbedarf - Datenschutzklasse 1

   [1]Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung keine besonders schwerwiegende Beeinträchtigung der betroffenen Person erwarten lässt. [2]Beispiele hierfür sind Namens- und Adressangaben ohne Sperrvermerke sowie Berufs-, Branchen- oder Geschäftsbezeichnungen, Geburts- und Jubiläumsdaten. [3]Abkündigungen im Gottesdienst.

2. Normaler Schutzbedarf - Datenschutzklasse 2

   [1]Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. [2]Beispiele hierfür sind Daten über wirtschaftliche Verhältnisse oder Umstände des persönlichen Lebens wie zum Beispiel, Mietverhältnisse, Geschäftsbeziehungen, Bescheide, die nicht Daten der Datenschutzklasse 3 enthalten. [3]Zu dieser Schutzkasse gehören ebenso Sitzungsprotokolle ohne Daten aus dem Beschäftigungsdatenschutz.

3. Hoher Schutzbedarf - Datenschutzklasse 3

   [1]Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. [2]Darunter fallen personenbezogene Daten besonderer Kategorien (§ 13 DSG-EKD), personenbezogene Daten, die dem Berufsgeheimnis unterliegen, deren Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann sowie personenbezogene Daten, die für Zwecke des Profiling verwendet werden können, insbesondere zur Analyse oder Prognose von Aspekten bezgl. [3]Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, den Aufenthaltsort oder Ortswechsel, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder

sie in ähnlicher Weise erheblich beeinträchtigt. [4]Beispiele hierfür sind genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung, strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln, personenbezogene Daten Schutzbedürftiger (z.B. Kinder), arbeitsrechtliche Rechtsverhältnisse, Sitzungsprotokolle mit Daten aus dem Beschäftigungsdatenschutz, Disziplinarentscheidungen, eindeutig identifizierende, hoch verknüpfbare Daten (z.B. Sozialversicherungsnummer, Steuer-ID).

4. Sehr hoher Schutzbedarf - Datenschutzklasse 4

   [1]Es handelt sich um personenbezogene Daten, bei der die Vertraulichkeit in höchstmöglichem Maß gewahrt bleiben muss, da eine Verletzung des Schutzes personenbezogener Daten ein hohes Schadensrisiko für die persönlichen Rechte natürlicher Personen zur Folge haben kann. [2]Betroffen hiervon sind personenbezogene Daten im Zusammenhang mit dem Beicht- und Seelsorgegeheimnis sowie Daten zur Aufarbeitung sexualisierter Gewalt nach § 50a DSG-EKD und Daten, die aktuelle Fälle der Grenzverletzungen nach der Gewaltschutzrichtlinie (GewSchR) betreffen.

(2) Zur Unterstützung der Datenschutzklassifizierung stellt der Evangelische Oberkirchenrat eine Anwenderrichtlinie zur Verfügung.

§ 4
Ablage von Daten

(1) Personenbezogene Daten mit geringem Schutzbedarf nach § 3 Abs. 1 Nr. 1 dürfen in Clouddiensten ohne besondere Verschlüsselung abgelegt werden.

(2) [1]Bei personenbezogenen Daten mit normalem Schutzbedarf nach § 3 Abs. 1 Nr. 2 ist eine Ablage in Clouddiensten ohne besondere Verschlüsselung gestattet. [2]Sollten jedoch spezifische IT-Fachsysteme für die Ablage dieser Daten zur Verfügung stehen, wie beispielsweise ein Dokumentenmanagement-System oder eine digitale Aktenführung, so ist die Verwendung dieser Fachsysteme aus Gründen des Datenschutzes verpflichtend und der Nutzung von Clouddiensten vorzuziehen.

(3) [1]Personenbezogene Daten mit hohem Schutzbedarf nach § 3 Nr. 3 dürfen in Clouddiensten nur dann abgelegt werden, wenn diese nach dem Stand der Technik zusätzlich geschützt sind. [2]Um diesen Schutz zu erreichen sind zwingend die von Microsoft 365 vorgegebenen Vertraulichkeitsbezeichnungen von Dokumenten und Ordnern im Rahmen der vom Evangelischen Oberkirchenrat zu erlassenden Anwenderrichtline (§ 3 Abs. 2) zur Informationsklassifizierung zu nutzen. [3]Durch die Vertraulichkeitsbezeichnung wird automatisiert eine Verschlüsselung anhand der Dokumentenklassifizierung durchgeführt. [4]Die Vorschrift des Absatz 2 Satz 2 ist anzuwenden.

(4) [1]Personenbezogene Daten mit sehr hohem Schutzbedarf (§ 3 Abs. 1 Nr. 4) nach § 3 DSG-EKD i.V.m. §§ 11 und 12 SeelGG.EKD und § 30 PfDG.EKD dürfen nur in

zusätzlich verschlüsselten Spezialcontainern auf lokalen dienstlichen Geräten abgelegt werden. [2]Eine Ablage in Clouddiensten ist untersagt. [3]Hierzu stellt der Evangelische Oberkirchenrat in der Anwenderrichtlinie nach § 3 Abs. 2 bezüglich des jeweils aktuellen Verschlüsselungsverfahrens Informationen bereit.

(5) [1]Personenbezogene Daten zur Aufarbeitung sexualisierter Gewalt (§ 3 Abs. 1 Nr. 4) gemäß § 50a DSG-EKD und die aktuellen Fälle der Grenzverletzungen nach GewSchR betreffen müssen in einem zentral bereitgestellten Spezialcontainer abgelegt werden, der von der IT-Abteilung des Evangelischen Oberkirchenrats zur Verfügung gestellt wird. [2]Der Zugriff über private Endgeräte auf diesen Spezialcontainer ist untersagt.

(6) [1]Der Zugriff von privaten Endgeräten auf personenbezogenen Daten der Datenschutzklassen nach § 3 Abs. 1 Nummern 2 und 3 über Clouddienste ist nur zulässig, wenn kein betriebliches Endgerät zur Verfügung steht. [2]Das Herunterladen von personenbezogenen Daten der Datenschutzklasse nach § 3 Abs. 1 Nummern 2 und 3 auf lokale Speicher in privaten Endgeräten ist untersagt.

§ 5
Sozialdatenschutz

Soweit die verantwortliche Stelle aufgrund staatlichen oder kirchlichen Rechts (§ 54 Abs. 3 DSG-EKD) verpflichtet ist, den Schutz von Sozialdaten i.S.d. § 67a SGB X zu gewährleisten, gelten für die Verarbeitung von personenbezogenen Daten die Bestimmungen der Sozialgesetzbücher in der jeweils aktuellen Fassung (§ 2 Abs. 6 DSG-EKD).

§ 6
Inkrafttreten, Außerkrafttreten

(1) Diese Durchführungsbestimmungen treten am 1. Januar 2025 in Kraft.

(2) Gleichzeitig treten die Durchführungsbestimmungen zur Datenablage in Clouddiensten
(DB-Ablage-Cloud) vom 05. September 2023 (GVBl., Nr. 77, S. 142) außer Kraft.