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

Vom 5. September 2023 (GVBl., Nr. 77, S. 142)
Außer Kraft getreten am 1. Januar 2025 (GVBl., Nr. 25, S. 72)

Der Evangelische Oberkirchenrat hat 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 erlassen:

§ 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 drei 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

   Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung keine besonders schwerwiegende Beeinträchtigung der betroffenen Person erwarten lässt. Beispiele hierfür sind Namens- und Adressangaben ohne Sperrvermerke sowie Berufs-, Branchen- oder Geschäftsbezeichnungen, Geburts- und Jubiläumsdaten. Ankündigungen im Gottesdienst, Sitzungsprotokolle ohne Daten aus dem Beschäftigungsdatenschutz.

2. Normaler Schutzbedarf - Datenschutzklasse 2

   Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Beispiele hierfür sind Daten über wirtschaftliche Verhältnisse oder Belange des persönlichen Lebens wie zum Beispiel Mietverhältnisse, Geschäftsbeziehungen, Bescheide, die nicht Daten der Datenschutzklasse 3 enthalten.

3. Hoher Schutzbedarf - Datenschutzklasse 3

   Es handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. 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. 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. 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, Disziplinarentscheidungen, eindeutig identifizierende, hoch verknüpfbare Daten (z.B. Sozialversicherungsnummer, Steuer-ID).

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

§ 4
Ablage von Daten

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

(2) [1]Bei personenbezogenen Daten mit normalem Schutzbedarf nach § 3 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, eine elektronische Personalakte oder eine digitale Aktenführung, so ist die Verwendung dieser Fachsysteme aus Gründen des Datenschutzes dringend zu empfehlen 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 und ein Zugriff durch Dienstanbieter technisch ausgeschlossen wird. [2]Zum Zeitpunkt des Inkrafttretens dieser Durchführungsbestimmungen sind keine praxistauglichen Verfahren marktreif, so dass eine Ablage nicht zulässig ist.

(4) [1]Der Zugriff von privaten Endgeräten auf personenbezogenen Daten der Datenschutzklassen nach § 3 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 Nummern 2 und 3 auf lokale Speicher in privaten Endgeräten ist untersagt.

§ 5
Besondere Sicherungsmaßnahmen, Seelsorgegeheimnis

(1) [1]Sobald Daten mit normalem oder hohem Schutzbedarf (§ 3 Nummern 2 oder 3) abgelegt werden, ist als Sicherungsmaßnahme für jeden Nutzer der Zugriff auf diese Daten durch die Aktivierung einer Multi-Faktor-Authentifizierung zu schützen, um ein ausreichendes Sicherungsniveau zu gewährleisten. [2]Andernfalls ist die Nutzung von Clouddiensten ausgeschlossen.

(2) [1]Der Umgang mit personenbezogenen Daten, die dem Seelsorgegeheimnis unterliegen, ist in besonders hohem Maße schutzbedürftig. [2]Eine Ablage dieser Daten in Clouddiensten ist nicht zulässig. [3]Ihre unzulässige Verarbeitung würde dem Vertrauen in die Verschwiegenheit der kirchlichen Rechtsträger schweren Schaden zufügen. [4]Personenbezogene Daten, die dem Seelsorgegeheimnis unterliegen, dürfen daher nur verarbeitet werden, wenn dem besonderen Schutzniveau angepasste, erforderlichenfalls über das Schutzniveau der Datenschutzklasse im Sinne von § 3 Nr. 3 hinausgehende technische und organisatorische Maßnahmen ergriffen werden.

§ 6
Inkrafttreten

Diese Durchführungsbestimmungen treten am 1. Oktober 2023 in Kraft.