

## **Verordnung zur Änderung der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO-Änderungsverordnung)**

### **Artikel 1**

#### **Änderung der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)**

Die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018 (Amtsblatt für die Diözese Augsburg 2019, Nr. 2 vom 19. Februar 2019, Seite 60 ff.) wird aufgrund des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 24. November 2025 wie folgt geändert:

#### **1. Die Inhaltsübersicht wird wie folgt neu gefasst:**

##### **„Inhaltsübersicht**

##### **Kapitel 1**

##### **Verarbeitungstätigkeiten**

§ 1 Verzeichnis von Verarbeitungstätigkeiten

##### **Kapitel 2**

##### **Datengeheimnis**

§ 2 Belehrung und Verpflichtung auf das Datengeheimnis, Schulung

§ 3 Inhalt der Verpflichtungserklärung

##### **Kapitel 3**

##### **Technische und organisatorische Maßnahmen**

##### **Abschnitt 1**

##### **Grundsätze und Maßnahmen**

§ 4 Begriffsbestimmungen (IT-Systeme, Lesbarkeit)

§ 5 Grundsätze der Verarbeitung

§ 6 Technische und organisatorische Maßnahmen

§ 7 Überprüfung

§ 8 Verarbeitung von Meldedaten in kirchlichen Rechenzentren

##### **Abschnitt 2**

##### **Schutzbedarf und Risikoanalyse**

§ 9 Einordnung in Datenschutzklassen und Datenschutzniveau

§ 10 Risikoanalyse

§ 11 Datenschutzklasse I und Schutzniveau I

§ 12 Datenschutzklasse II und Schutzniveau II

§ 13 Datenschutzklasse III und Schutzniveau III

§ 14 Umgang mit personenbezogenen Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen

## **Kapitel 4**

### **Maßnahmen des Verantwortlichen und des oder der Mitarbeitenden**

- § 15 Maßnahmen des Verantwortlichen
- § 16 Maßnahmen des Verantwortlichen zur Datensicherung
- § 17 Maßnahmen des oder der Mitarbeitenden

## **Kapitel 5**

### **Besondere Gefahrenlagen**

- § 18 Nutzung von Cloud-Diensten
- § 19 Autorisierte Programme
- § 20 Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken
- § 21 Nutzung privater IT-Systeme zu dienstlichen Zwecken
- § 22 Externe Zugriffe, Auftragsverarbeitung
- § 23 Verschrottung und Vernichtung von IT-Systemen, Abgabe von IT-Systemen zur weiteren Nutzung
- § 24 Passwortlisten der Systemverwaltung
- § 25 Übermittlung personenbezogener Daten per Fax
- § 26 Sonstige Formen der Übermittlung personenbezogener Daten
- § 27 Kopier-/Scangeräte

## **Kapitel 6**

### **Übergangs- und Schlussbestimmungen**

- § 28 Inkrafttreten“

#### **2. § 1 wird wie folgt geändert:**

- a) In Absatz 1 werden nach dem Wort „dem“ die Wörter „oder der“ und nach dem Wort „solcher“ die Wörter „oder eine solche“ angefügt.
- b) Der bisherige Absatz 2 wird ersatzlos gestrichen.
- c) Der bisherige Absatz 3 wird Absatz 2.
- d) Der bisherige Absatz 4 wird ersatzlos gestrichen.
- e) Der bisherige Absatz 5 wird Absatz 3.
- f) Absatz 3 Satz 3 wird wie folgt neu gefasst:  
„Die Überprüfung sowie die Aktualisierung sind in geeigneter Weise zu dokumentieren.“

#### **3. § 2 wird wie folgt geändert:**

- a) In der Überschrift werden nach dem Wort „Datengeheimnis“ ein Komma sowie das Wort „Schulung“ angefügt.
- b) In Absatz 1 wird der Klammerzusatz wie folgt neu gefasst:  
„(Mitarbeitende im Sinne dieser Durchführungsverordnung, im Folgenden: Mitarbeitende)“.
- c) In Absatz 2 Satz 1 wird das Wort „Mitarbeiter“ durch das Wort „Mitarbeitenden“ ersetzt.
- d) In Absatz 2 Satz 3 wird das Wort „Mitarbeitern“ durch das Wort „Mitarbeitenden“ ersetzt.
- e) In Absatz 3 wird das Wort „Mitarbeiter“ ersetzt durch das Wort „Mitarbeitenden“.
- f) In Absatz 4 werden die Wörter „der Mitarbeiter“ durch die Wörter „der Mitarbeitenden“ und die Wörter „den Mitarbeiter“ durch die Wörter „den Mitarbeitenden oder die Mitarbeitende“ ersetzt.

- g) In Absatz 5 Satz 1 wird das Wort „Mitarbeiter“ durch das Wort „Mitarbeitenden“ ersetzt.
- h) In Absatz 5 Satz 2 werden die Wörter „des jeweiligen Mitarbeiters“ durch die Wörter „des oder der Mitarbeitenden“ ersetzt.
- i) In Absatz 5 Satz 3 werden nach dem Wort „Dieser“ die Wörter „oder diese“ angefügt.
- j) In Absatz 6 werden nach dem Wort „Datengeheimnis“ die Wörter „gemäß § 5 KDG“ angefügt.
- k) Es wird folgender Absatz 7 angefügt:  
„Die Mitarbeitenden sind regelmäßig zu schulen.“

#### **4. § 3 wird wie folgt geändert:**

- a) In Absatz 1 erster Halbsatz wird das Wort „Mitarbeiters“ durch die Wörter „oder der Mitarbeitenden“ ersetzt.
- b) In Absatz 1 Buchstabe a) wird das Wort „Mitarbeiters“ durch die Wörter „oder der Mitarbeitenden“ ersetzt.
- c) In Absatz 1 Buchstabe b) werden das Wort „Mitarbeiter“ durch die Wörter „oder die Mitarbeitende“ ersetzt und nach dem Wort „seiner“ die Wörter „oder ihrer“ angefügt.
- d) In Absatz 1 Buchstabe c) wird das Wort „Mitarbeiters“ durch die Wörter „oder der Mitarbeitenden“ ersetzt.
- e) In Absatz 1 Buchstabe d) werden das Wort „Mitarbeiter“ durch die Wörter „oder die Mitarbeitende“ ersetzt und nach dem Wort „seiner“ die Wörter „oder ihrer“ angefügt.
- f) In Absatz 2 wird das Wort „Mitarbeiter“ durch die Wörter „oder der Mitarbeitenden“ ersetzt.
- g) Der bisherige Absatz 3 Satz 2 wird ersatzlos gestrichen.

#### **5. § 4 wird wie folgt neu gefasst:**

### **„§ 4 Begriffsbestimmungen (IT-Systeme, Lesbarkeit)“**

- (1) IT-Systeme im Sinne dieser Durchführungsverordnung sind sämtliche technischen Einrichtungen, mittels derer personenbezogene Daten automatisiert verarbeitet werden.
- (2) IT-Systeme sind insbesondere
  - a) hardwarebasierte IT-Komponenten (elektronische Geräte wie Server, Arbeitsplatzrechner, mobile Endgeräte, eingebettete Systeme (z. B. IoT) oder vergleichbare technische Komponenten, die einzeln oder im Verbund betrieben werden können),
  - b) Softwarelösungen (lokal installierte oder netzwerkgestützte Programme und Anwendungen einschließlich betriebssystemnaher Software und Anwendungssoftware, die unmittelbar oder mittelbar an der Verarbeitung personenbezogener Daten beteiligt sind),
  - c) cloudbasierte Systeme und Dienste (Bereitstellungsformen wie Software as a Service (SaaS), Platform as a Service (PaaS) oder Infrastructure as a Service (IaaS), die über netzwerkbasierte Umgebungen (insbesondere Internet oder Intranet) zugänglich sind und zur Datenverarbeitung eingesetzt werden).
- (3) Unter Lesbarkeit im Sinne dieser Durchführungsverordnung ist die Möglichkeit zur vollständigen oder teilweisen Wiedergabe des Informationsgehalts von personenbezogenen Daten zu verstehen.“

## **6. § 6 wird wie folgt geändert:**

- a) In Absatz 1 Buchstabe b) wird der Klammerzusatz wie folgt neu gefasst:  
„(z. B. durch Verschlüsselung mit geeigneten Verschlüsselungsverfahren; das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen)“.
- b) In Absatz 2 werden nach dem Wort „Form“ die Wörter „unabhängig vom Ort der Verarbeitungstätigkeit“ angefügt.
- c) In Absatz 2 Buchstabe a) werden nach dem Wort „IT-Systemen“ die Wörter „im Sinne des § 4 Absatz 2 Nr. 1“ angefügt.
- d) Absatz 2 Buchstabe b) wird wie folgt neu gefasst:  
„<sup>1</sup>Es ist zu verhindern, dass IT-Systeme und Benutzerzugänge von Unbefugten genutzt werden können (Zugangskontrolle). <sup>2</sup>Zum Schutz personenbezogener Daten und zur Vermeidung von Identitätsdiebstahl sind geeignete technische und organisatorische Maßnahmen nach dem jeweiligen Stand der Technik zu ergreifen. <sup>3</sup>Dies gilt insbesondere für Datenverarbeitungen außerhalb eines geschlossenen und gesicherten Netzwerks.“
- e) In Absatz 2 Buchstabe i) wird nach dem Wort „erhobene“ das Wort „personenbezogene“ angefügt.
- f) Nach Absatz 2 Buchstabe j) wird folgender Buchstabe k) angefügt:  
„Bei der Auswahl von IT-Systemen, insbesondere von Softwarelösungen, ist dem Grundsatz der Datenminimierung angemessen Rechnung zu tragen.“
- g) Absatz 3 wird wie folgt neu gefasst:  
„Absatz 2 gilt entsprechend für die Verarbeitung personenbezogener Daten in nicht automatisierter Form.“

## **7. § 7 Absatz 2 wird wie folgt neu gefasst:**

„<sup>1</sup>Insbesondere die Vorlage eines anerkannten Zertifikats gemäß § 26 Absatz 4 KDG durch den Verantwortlichen, welches sich an Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert, ist als Nachweis zulässig. <sup>2</sup>Abweichend von Satz 1 kann auch eine Orientierung an anderen Regelungen erfolgen, die einen vergleichbaren Schutzstandard gewährleisten (insbesondere ISO/IEC 27001).“

## **8. § 8 Absatz 2 wird wie folgt geändert:**

Das Wort „Vorschrift“ wird durch das Wort „Durchführungsverordnung“ ersetzt.

## **9. § 9 wird wie folgt neu gefasst:**

### **„§ 9**

#### **Einordnung in Datenschutzklassen und Datenschutzniveau**

- (1) Unter Berücksichtigung der Art der zu verarbeitenden personenbezogenen Daten und des Ausmaßes der möglichen Gefährdung personenbezogener Daten hat eine Einordnung in eine der in §§ 11 bis 13 genannten drei Datenschutzklassen zu erfolgen.
- (2) 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.
- (3) <sup>1</sup>Die Einordnung erfolgt durch den Verantwortlichen; sie soll in der Regel bei Erstellung des Verzeichnisses von Verarbeitungstätigkeiten vorgenommen werden. <sup>2</sup>Der oder die betriebliche Datenschutzbeauftragte soll angehört werden.

- (4) <sup>1</sup>In begründeten Einzelfällen kann der Verantwortliche eine abweichende Einordnung vornehmen. <sup>2</sup>Die Gründe sind zu dokumentieren. <sup>3</sup>Erfolgt eine Einordnung in eine niedrigere Datenschutzklasse, ist zuvor der oder die betriebliche Datenschutzbeauftragte anzuhören.
- (5) Erfolgt keine Einordnung, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen des § 14 vorliegen.
- (6) Die Einordnung in eine der nachfolgend genannten Datenschutzklassen erfordert die Einhaltung des dieser Datenschutzklasse entsprechenden Schutzniveaus und die Einhaltung der dort beschriebenen Mindestmaßnahmen.
- (7) Erfolgt die Verarbeitung durch einen Auftragsverarbeiter, ist der Verantwortliche verpflichtet, sich in geeigneter Weise, insbesondere durch persönliche Überprüfung oder Vorlage von Nachweisen, von dem Bestehen des der jeweiligen Datenschutzklasse entsprechenden Schutzniveaus zu überzeugen.“

#### **10. § 10 wird wie folgt neu gefasst:**

##### **„§ 10 Risikoanalyse**

- (1) Die den individuellen Gegebenheiten entspringenden Risiken sind vom Verantwortlichen anhand einer Risikoanalyse festzustellen.
- (2) <sup>1</sup>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. <sup>2</sup>Hierzu zählen insbesondere die Eintrittswahrscheinlichkeit und die Schwere eines Schadens für die betroffene Person. <sup>3</sup>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) Die identifizierten Risiken sind durch entsprechende Maßnahmen im Einklang mit § 6 zu behandeln.“

#### **11. § 11 wird wie folgt geändert:**

- a) Absatz 2 Buchstabe b) wird wie folgt neu gefasst:  
„<sup>1</sup>Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Passwortes oder unter Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens zulässig. <sup>2</sup>In sicherheitskritischen Bereichen oder bei Zugriffen außerhalb gesicherter Netze ist insbesondere der Einsatz von Mehr-Faktor-Authentifizierungsverfahren (z. B. Kombination aus Passwort und Einmalcode, Hardware-Token oder biometrischen Verfahren) vorzusehen.“
- b) Absatz 2 Buchstabe c) wird wie folgt neu gefasst:  
„Sicherungskopien von Daten sind nach aktuellem Stand der Technik mit geeigneten Maßnahmen vor unbefugtem Zugriff zu schützen.“

#### **12. § 12 wird wie folgt geändert:**

- a) Absatz 2 Buchstabe a) wird wie folgt neu gefasst:  
„<sup>1</sup>Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Passwortes zulässig, das ausreichend komplex gewählt werden muss und dessen Erneuerung nach dem jeweiligen Sicherheitsbedarf erfolgt. <sup>2</sup>Alternativ ist die Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens

zulässig.“

- b) In Absatz 2 Buchstabe b) wird nach Satz 1 folgender Satz 2 angefügt:  
„Zu diesem Zweck sind geeignete technische Maßnahmen wie beispielsweise ein Boot-Schutz umzusetzen.“
- c) In Absatz 2 Buchstabe d) Satz 2 werden nach dem Wort „dem“ die Wörter „oder der“ angefügt.

### **13. § 14 wird wie folgt geändert:**

- a) Die Überschrift wird wie folgt neu gefasst:  
„Umgang mit personenbezogenen Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen“
- b) In Absatz 1 werden die Wörter „Beicht- oder Seelsorgegeheimnis“ ersetzt durch die Wörter „Beichtgeheimnis oder dem Seelsorgegeheimnis“.
- c) Absatz 5 wird wie folgt neu gefasst:  
„Erfolgt die Seelsorge außerhalb eines geschlossenen Netzwerkes, sind geeignete, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende, technische und organisatorische Maßnahmen nach dem aktuellen Stand der Technik zu treffen.“

### **14. Die Überschrift von Kapitel 4 wird wie folgt geändert:**

Das Wort „Mitarbeiters“ wird ersetzt durch die Wörter „oder der Mitarbeitenden“.

### **15. § 15 wird wie folgt geändert:**

- a) In Absatz 3 werden die Wörter „seine Mitarbeiter“ ersetzt durch die Wörter „die Mitarbeitenden“.
- b) In Absatz 4 wird der Klammerzusatz „(Datenschutzkonzept)“ ersatzlos gestrichen.
- c) In Absatz 6 Satz 1 wird das Wort „Mitarbeiter“ durch das Wort „Mitarbeitende“ ersetzt.
- d) In Absatz 6 Satz 2 werden hinter dem Wort „Datenschutzbeauftragten“ die Wörter „oder die betriebliche Datenschutzbeauftragte“ angefügt.

### **16. § 17 wird wie folgt geändert:**

- a) Die Überschrift wird wie folgt neu gefasst:  
„Maßnahmen des oder der Mitarbeitenden“
- b) In Satz 1 werden die Wörter „jeder Mitarbeiter“ ersetzt durch die Wörter „jeder und jede Mitarbeitende“.
- c) In Satz 2 werden hinter dem Wort „ihm“ die Wörter „oder ihr“ angefügt.

### **17. In Kapitel 5 wird folgender § 18 neu eingefügt:**

#### **„§ 18**

#### **Nutzung von Cloud-Diensten**

Für die Verarbeitung personenbezogener Daten mit einem Cloud-Dienst gilt ergänzend zu den Vorschriften der §§ 5 ff.:

- (1) Es sind primär bereits geprüfte und freigegebene Cloud-Dienste zu nutzen.
- (2) <sup>1</sup>Vor der Nutzung anderer Cloud-Dienste ist anhand nachfolgender Aspekte zu prüfen, ob die erforderlichen Sicherheitsanforderungen erfüllt werden. <sup>2</sup>Folgende Aspekte können ein erhöhtes Risiko darstellen:

- a) ungeplante vorzeitige Vertragsbeendigung durch den Diensteanbieter,
  - b) unzureichend gesicherte administrative Zugänge,
  - c) mangelnde Portabilität von personenbezogenen Daten und IT-Systemen,
  - d) generelle Abhängigkeit vom Cloud-Diensteanbieter mangels Wechselmöglichkeit,
  - e) Gefährdung der Integrität von Informationen aufgrund herstellerspezifischer Datenformate,
  - f) gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Kunden,
  - g) Unkenntnis über den Speicherort der Informationen,
  - h) hohe Mobilität der Informationen sowie
  - i) unbefugter Zugriff auf Informationen beispielsweise durch Administrationspersonal des Cloud-Diensteanbieters oder Dritte.
- (3) Vor der Nutzung des Cloud-Dienstes ist in Abhängigkeit von der Risikoanalyse eine Exit-Strategie zu definieren (z. B. Datenlöschung, Datenübertragung).“

**18. Der bisherige § 18 wird § 19.**

**19. Der bisherige § 19 wird § 20.**

**20. Der bisherige § 20 wird § 21.**

**21. Der neue § 21 wird wie folgt geändert:**

- a) In Absatz 2 Satz 1 Buchstabe b) wird das Wort „Mitarbeiters“ ersetzt durch die Wörter „oder der Mitarbeitenden“.
- b) In Absatz 2 Satz 2 werden die Wörter „betreffenden Mitarbeiter“ ersetzt durch die Wörter „oder der betreffenden Mitarbeitenden“.
- c) In Absatz 3 wird das Wort „Mitarbeitern“ ersetzt durch das Wort „Mitarbeitenden“.
- d) Absatz 4 wird wie folgt neu gefasst:  
 „<sup>1</sup>Die Weiterleitung dienstlicher personenbezogener Daten auf private E-Mail-Konten ist unzulässig. <sup>2</sup>Dies gilt auch für personalisierte E-Mail-Adressen. <sup>3</sup>Ausnahmeregelungen können von dem Verantwortlichen getroffen werden, soweit das datenschutzrechtliche Schutzniveau, insbesondere nach dem KDG oder dieser Durchführungsverordnung, nicht unterschritten wird.“
- e) Nach Absatz 4 wird folgender Absatz 5 neu angefügt:  
 „Der oder die Mitarbeitende hat sicherzustellen, dass unberechtigte Dritte, insbesondere Familienmitglieder, keinen Zugriff auf dienstliche personenbezogene Daten haben.“

**22. Der bisherige § 21 wird § 22.**

**23. Im neuen § 22 wird Absatz 5 wie folgt neu gefasst:**

„<sup>1</sup>Eine Fernwartung von IT-Systemen darf darüber hinaus nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde, über sichere Verbindungen erfolgt und die Fernwartung systemseitig protokolliert wird. <sup>2</sup>Im Falle der Einbeziehung externer Dienstleister sind auch die datenschutzrechtlichen Anforderungen und Verantwortlichkeiten sowie technische Schutzmaßnahmen vertraglich zu regeln.“

**24. Der bisherige § 22 wird § 23.**

**25. Der neue § 23 wird wie folgt geändert:**

In Absatz 1 Satz 1 werden nach dem Wort „IT-Systemen“ die Wörter „im Sinne des § 4

Absatz 2 Nr. 1 dieser Verordnung“ angefügt.

**26. Der bisherige § 23 wird § 24.**

**27. Der bisherige § 24 wird § 25.**

**28. Der neue § 25 wird wie folgt neu gefasst:**

**„§ 25**

**Übermittlung personenbezogener Daten per Fax**

<sup>1</sup>Die Übermittlung personenbezogener Daten per Fax ist grundsätzlich unzulässig. <sup>2</sup>In spezifischen Bestimmungen können Ausnahmen, insbesondere Übergangsbestimmungen, vorgesehen werden; dabei sind die Vorschriften der §§ 5 ff. und die jeweils aktuellen Sicherheitsstandards zu beachten.“

**29. Der bisherige § 25 wird § 26.**

**30. Im neuen § 26 wird in Absatz 1 nach Satz 1 folgender Satz 2 angefügt:**

„Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.“

**31. Der bisherige § 26 wird § 27.**

**32. Der neue § 27 wird wie folgt geändert:**

Das Wort „Mitarbeiter“ wird ersetzt durch das Wort „Mitarbeitende“.

**33. Der bisherige § 27 wird ersatzlos gestrichen.**

**34. § 28 wird wie folgt neu gefasst:**

**„§ 28**

**Inkrafttreten**

Diese Durchführungsverordnung tritt zum 01.03.2026 in Kraft.“

**Artikel 2**

**Inkrafttreten**

Diese Änderungsverordnung tritt am 01.03.2026 in Kraft.

Augsburg, 13. Januar 2026.

Dr. Wolfgang Hacker  
Generalvikar

Kathrin Rommel  
Notarin