

# **Verordnung zur Verarbeitung personenbezogener Daten im Auftrag nach § 29 des Gesetzes über den Kirchlichen Datenschutz (§ 29 KDG-VO)**

**Vom 7. Oktober 2020**

ABl. EBK 2020, Nr. 145, S. 156

Aufgrund des § 2 des Gesetzes zur Verarbeitung personenbezogener Daten im Auftrag nach § 29 KDG (§ 29-KDG-Gesetz)\*<sup>1</sup> wird folgende Verordnung erlassen:

## **§ 1**

### **Anwendungsbereich**

Diese Verordnung gilt für die Verarbeitung personenbezogener Daten im Auftrag durch kirchliche Stellen (Verarbeiter) für andere kirchliche Stellen (Verantwortlicher) im Sinne von § 1 § 29-KDG-Gesetz.

## **§ 2**

### **Gegenstand der Auftragsverarbeitung; Dauer der Verarbeitung**

- (1) Für den Gegenstand der Auftragsverarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und die Kategorien der durch die Verarbeitung betroffenen Personen wird auf die Anlage zu dieser Verordnung verwiesen.\*<sup>2</sup>
- (2) Die Verarbeitung erfolgt unbefristet und endet spätestens mit dem ersatzlosen Außerkrafttreten dieser Verordnung.
- (3) <sup>1</sup>Die Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. <sup>2</sup>Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 39 ff. KDG erfüllt sind.

## **§ 3**

### **Technisch-organisatorische Maßnahmen**

- (1) <sup>1</sup>Der Verarbeiter hat die Umsetzung der im Vorfeld der Verarbeitung dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Durchführung zu dokumentieren und dem Verantwortlichen auf Nachfrage zur Prüfung zu übergeben. <sup>2</sup>Soweit eine Prüfung/ein

---

\*<sup>1</sup> (Amtsblatt des Erzbistum Köln 2020 Nr. 141 im selben Heft)

\*<sup>2</sup> (Amtsblatt des Erzbistum Köln 2020 Nr. 146 im selben Heft)

Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) <sup>1</sup>Der Verarbeiter hat die Sicherheit gem. §§ 29 Abs. 4 lit. c, 26 KDG insbesondere in Verbindung mit § 7 Abs. 1 und 2 KDG und den einschlägigen Regelungen der jeweils geltenden KDG-DVO herzustellen. <sup>2</sup>Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. <sup>3</sup>Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von § 26 Abs. 1 und 3 KDG zu berücksichtigen.

(3) <sup>1</sup>Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. <sup>2</sup>Insoweit ist es dem Verarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. <sup>3</sup>Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. <sup>4</sup>Wesentliche Änderungen sind zu dokumentieren.

#### § 4

##### **Berichtigung, Einschränkung und Löschung von Daten**

(1) <sup>1</sup>Der Verarbeiter darf die Daten, die verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. <sup>2</sup>Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Verarbeiter wendet, wird der Verarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(2) Soweit vom Gegenstand der Verarbeitung umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Verarbeiter sicherzustellen.

#### § 5

##### **Qualitätssicherung und sonstige Pflichten des Verarbeiters**

Der Verarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieser Verordnung gesetzliche Pflichten gemäß §§ 26, 29 bis 33 KDG; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) <sup>1</sup>Benennung eines betrieblichen Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 37, 38 KDG ausübt. <sup>2</sup>Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt. <sup>3</sup>Ein Wechsel des betrieblichen Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.

- b) 1Die Wahrung der Vertraulichkeit gemäß §§ 26 Abs. 5, 29 Abs. 4 lit. b, 30 KDG.  
2Der Verarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit gemäß § 5 KDG verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. 3Der Verarbeiter und jede dem Verarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in dieser Verordnung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Die Umsetzung und Einhaltung aller für die Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen gemäß §§ 29 Abs. 4 lit. c, 26 KDG.
- d) Der Verantwortliche und der Verarbeiter arbeiten auf Anfrage mit der kirchlichen Datenschutzaufsicht bei der Erfüllung ihrer Aufgaben zusammen.
- e) 1Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der kirchlichen Datenschutzaufsicht, soweit sie sich auf diese Verarbeitung beziehen. 2Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Verarbeitung beim Verarbeiter ermittelt.
- f) Soweit der Verantwortliche seinerseits einer Kontrolle der kirchlichen Datenschutzaufsicht, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Verarbeitung beim Verarbeiter ausgesetzt ist, hat ihn der Verarbeiter nach besten Kräften zu unterstützen.
- g) Der Verarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollrechte nach § 7 dieser Verordnung.

## § 6

### Unterauftragsverarbeitung

- (1) 1Als Unterauftragsverarbeitung im Sinne dieser Verordnung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf den Gegenstand der Verarbeitung beziehen. 2Nicht hierzu gehören Nebenleistungen, die der Verarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der

Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. <sup>3</sup>Der Verarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Verarbeiter legt dem Verantwortlichen auf Anforderung zu Beginn der Verarbeitung eine Liste der Unterverarbeiter oder Unterverarbeiterkategorien vor und unterrichtet ihn unverzüglich bei etwaigen Änderungen (mindestens in Textform).

(3) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterverarbeitung gestattet.

(4) <sup>1</sup>Erbringt der Unterverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt der Verarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. <sup>2</sup>Gleiches gilt, wenn Dienstleister eingesetzt werden sollen.

(5) <sup>1</sup>Eine weitere Auslagerung durch den Unterverarbeiter bedarf der ausdrücklichen Zustimmung des Verarbeiters (mindestens in Textform). <sup>2</sup>Sämtliche Regelungen dieser Verordnung sind auch dem weiteren Unterverarbeiter aufzuerlegen.

## § 7

### **Kontrollrechte des Verantwortlichen**

(1) <sup>1</sup>Der Verantwortliche hat das Recht, im Benehmen mit dem Verarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. <sup>2</sup>Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Verordnung durch den Verarbeiter zu überzeugen.

(2) <sup>1</sup>Der Verarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Verarbeiters nach § 29 KDG überzeugen kann. <sup>2</sup>Der Verarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur die konkrete Verarbeitung betreffen, kann, soweit einschlägig, erfolgen durch

- a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO,
- b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO,
- c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), oder

- d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz).

## § 8

### Mitteilung bei Verstößen des Verarbeiters

1Der Verarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den §§ 26, 33 bis 35 KDG genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. 2Hierzu gehören u.a.:

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden;
- c) die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen;
- d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgeabschätzung;
- e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der kirchlichen Datenschutzaufsicht.

## § 9

### Weisungsbefugnis des Verantwortlichen

(1) Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mindestens in Textform).

(2) 1Der Verarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. 2Der Verarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

## § 10

### Löschung und Rückgabe von personenbezogenen Daten

(1) 1Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. 2Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) <sup>1</sup>Nach Beendigung der Verarbeitung oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit ersatzlosem Außerkrafttreten dieser Verordnung, sofern nicht eine Vereinbarung nach § 29 KDG getroffen wurde - hat der Verarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Verarbeitung stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. <sup>2</sup>Gleiches gilt für Test- und Ausschussmaterial. <sup>3</sup>Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) <sup>1</sup>Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Verarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über die Beendigung der Verarbeitung hinaus aufzubewahren. <sup>2</sup>Er kann sie zu seiner Entlastung bei Beendigung der Verarbeitung dem Verantwortlichen übergeben.

## § 11

### **Inkrafttreten**

Diese Verordnung tritt zum 1. November 2020 in Kraft.