

**Gesetz zur Regelung des Rechts-
instruments nach § 29 Gesetz über
den Kirchlichen Datenschutz (KDG)
im Bereich der Diözese Aachen
(§ 29-KDG-Gesetz)**

vom 10. September 2019

**Verordnung zur Durchführung des
Gesetzes zur Regelung des Rechts-
instruments nach § 29 Gesetz über
den Kirchlichen Datenschutz (KDG)
im Bereich der Diözese Aachen
(§ 29-KDG-Gesetz-DVO)**

vom 24. Februar 2022



Katholisches
Datenschutzzentrum

Gesetz zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG) im Bereich der Diözese Aachen (§ 29-KDG-Gesetz)

Seite 3

Verordnung zur Durchführung des Gesetzes zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG) im Bereich der Diözese Aachen (§ 29-KDG-Gesetz-DVO)

Seite 5

nichtamtliche Lesefassungen

Gesetz vom 10. September 2019

veröffentlicht im Amtsblatt Nr. 10 vom 01. Oktober 2019

Verordnung vom 24. Februar 2022

veröffentlicht im Amtsblatt Nr. 4 vom 01. April 2022

Herausgeber:

Diözesandatenschutzbeauftragter für die Erzdiozesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und Verbandsdatenschutzbeauftragter des Verbandes der Diözesen Deutschlands (VDD)

Steffen Pau

Katholisches Datenschutzzentrum (KdöR)

Brackeler Hellweg 144

44309 Dortmund

Tel. 0231 / 13 89 85 – 0

Fax 0231 / 13 89 85 – 22

E-Mail: info@kdsz.de

www.katholisches-datenschutzzentrum.de

Gesetz zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG) im Bereich der Diözese Aachen (§ 29-KDG-Gesetz)

Zur Regelung des Rechtsinstruments nach § 29 KDG über die Verarbeitung personenbezogener Daten im Auftrag wird das nachfolgende Gesetz erlassen.

§ 1

Anwendungsbereich

Dieses Gesetz gilt für kirchliche Stellen im Bereich der Diözese Aachen, die im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind. Hierzu gehören neben der Diözese insbesondere der Bischöfliche Stuhl, das Domkapitel, die Kirchengemeindeverbände und Kirchengemeinden. Es gilt auch für die sonstigen öffentlich-rechtlich verfassten selbstständigen Vermögensmassen auf Ortskirchenebene, insbesondere die Fabrik- und Stellenvermögen.

§ 2

Verarbeitung personenbezogener Daten im Auftrag

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt gemäß § 29 Absatz 3 KDG aufgrund eines Vertrages oder aufgrund dieses Gesetzes. Hierbei sind insbesondere die Vorgaben nach § 29 Absatz 3 und 4 KDG zu beachten.

§ 3

Regelung durch Verwaltungsverordnung

Die zur Durchführung dieses Gesetzes erforderlichen Regelungen trifft der Generalvikar.

§ 4

Schlussbestimmungen

Dieses Gesetz tritt zum 01. Oktober 2019 in Kraft.

Aachen, 10. September 2019

† Dr. Helmut Dieser
Bischof von Aachen

Verordnung zur Durchführung des Gesetzes zur Regelung des Rechtsinstruments nach § 29 Gesetz über den Kirchlichen Datenschutz (KDG) im Bereich der Diözese Aachen (§ 29-KDG-Gesetz-DVO)

Aufgrund des § 3 des Gesetzes zur Regelung des Rechtsinstruments nach § 29 KDG über die Verarbeitung personenbezogener Daten im Auftrag wird folgende Verordnung erlassen:

§ 1

Gegenstand der Verordnung, Dauer der Verarbeitung

- (1) Gegenstand dieser Verordnung ist die Schaffung einer Grundlage für die Verarbeitung personenbezogener Daten durch eine kirchliche Stelle für eine andere kirchliche Stelle. Beteiligte können sein das Bistum Aachen, der Bischöfliche Stuhl in Aachen, das Domkapitel in Aachen, die Kirchengemeindeverbände, die Kirchengemeinden und sonstige öffentlich-rechtlich verfasste kirchliche Stellen für andere öffentlich-rechtlich verfasste kirchliche Stellen im Bistum Aachen jeweils entweder als Verantwortlicher oder als Verarbeiter im Sinne des KDG. Sie gilt für jede Verarbeitung personenbezogener Daten, soweit eine der genannten Beteiligten diese Daten für eine der anderen genannten Beteiligten verarbeitet.
- (2) Die Verarbeitung umfasst insbesondere folgende Aufgaben:
Bereitstellung von Anwendungssoftware, Tätigkeiten und Diensten im Rahmen folgender exemplarischer Verarbeitungen:
 - Personalverwaltung und –abrechnung,
 - Finanzbuchhaltung,
 - Immobilienverwaltung,
 - Friedhofsverwaltung,
 - zentrale IT-Systeme (E-Mailsystem, Dateiablagensysteme, Archivierungssysteme, IT-Sicherheitssysteme, IT-Verwaltungssysteme),
 - kirchliches Meldewesen,
 - Verwaltungsaufgaben für Tageseinrichtungen für Kinder,
 - Verwaltungsaufgaben für Kirchengemeinden,
 - Plattformen für Onlineschulungen, Datenschutz Tätigkeiten,
 - Schulungen, Aus-, Fort- und Weiterbildungen.

- (3) Die Verarbeitung erfolgt unbefristet, soweit nicht vertraglich anderes vereinbart ist und endet spätestens mit dem ersatzlosen Außerkrafttreten dieser Verordnung.

§ 2

Konkretisierung des Auftragsinhalts

- (1) Nähere Beschreibung der Verarbeitung im Hinblick auf Art und Zweck der Aufgaben des Verarbeiters: Bereitstellung, Administration, Betrieb, Durchführung, Betreuung und weitere Tätigkeiten im Zusammenhang mit den in § 1 Abs. 2 genannten Arten der Verarbeitung zur Sicherstellung der ordnungsgemäßen Verwaltungstätigkeit der in § 1 Abs. 1 genannten Beteiligten.
- (2) Die dafür notwendigen Verarbeitungen sind im Rahmen einer konkretisierenden Vereinbarung, einem Gesetz, oder einer Verordnung genauer zu beschreiben.
- (3) Die Verarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. 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.
- (4) Gegenstand der Verarbeitung personenbezogener Daten sind je nach vorliegender Verarbeitung insbesondere folgende Datenarten/-kategorien:
 - Personenstammdaten (z.B. Namen, Geburtsdaten, Anschrift)
 - Kommunikationsdaten (z.B. Telefon, E-Mail)
 - Daten zur Personalverwaltung (z.B. Vergütung, Sozialdaten)
 - Vertragsstammdaten (z.B. Vertragsbeziehung, Vertragsinteresse)
 - Vertragsabrechnungs- und Zahlungsdaten
 - Planungs- und Steuerungsdaten
 - kirchliche und kommunale Meldedaten (gemäß Bundesmeldegesetz)
 - Daten für die Verwaltung von Tageseinrichtungen für Kinder
 - personenbezogene Vorgangsdaten in Akten

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitglieder und ggfs. deren Familienangehörige
- Mitarbeitende im Sinne des § 2 Abs. 1 KGDVO
- Vertragsparteien, Nutzungsberechtigte
- Abonnenten/Innen, Lieferanten/Innen, Kunden
- Ansprechpersonen

§ 3

Technisch-organisatorische Maßnahmen

- (1) 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. Soweit eine Prüfung/ ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) 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. 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. 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) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Verarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4

Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Verarbeiter darf die Daten, die verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. 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) Benennung eines betrieblichen Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 37, 38 KDG ausübt. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des betrieblichen Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.
- b) Die Wahrung der Vertraulichkeit gemäß §§ 26 Abs. 5, 29 Abs. 4 lit. b, 30 KDG. Der Verarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der 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) Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der kirchlichen Datenschutzaufsicht, soweit sie sich auf diese Verarbeitung beziehen. Dies 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) Als Unterauftragsverarbeitung im Sinne dieser Verordnung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf den Gegenstand der Verarbeitung beziehen. Nicht 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 Datenverarbeitungs-

anlagen in Anspruch nimmt. 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 vor und unterrichtet ihn bei etwaigen Änderungen (mindestens 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) Erbringt der Unterverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt der Verarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (5) Eine weitere Auslagerung durch den Unterverarbeiter bedarf der ausdrücklichen Zustimmung des Verarbeiters (mind. Textform). Sämtliche Regelungen dieser Verordnung sind auch dem weiteren Unterverarbeiter aufzuerlegen.

§ 7

Kontrollrechte des Verantwortlichen

- (1) Der Verantwortliche hat das Recht, im Benehmen mit dem Verarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. 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) Der Verarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Verarbeiters nach § 29 KDG überzeugen kann. 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);
 - d) eine geeignete Zertifizierung durch IT-Sicherheitsoder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 8

Mitteilung bei Verstößen des Verarbeiters

Der 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. Hierzu 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, den Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
- 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) Der Verarbeiter hat den Verantwortlichen zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der 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) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon 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) 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. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) 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. Er kann sie zu seiner Entlastung bei Beendigung der Verarbeitung dem Verantwortlichen übergeben.

§ 11

Inkrafttreten

Diese Verordnung tritt zum 1. April 2022 in Kraft.

Aachen, 24. Februar 2022

Dr. Andreas Frick
Generalvikar

