Verordnung
zur Durchführung des Gesetzes über die Auftragsdatenverarbeitung zwischen juristischen Personen im Erzbistum Hamburg

Vom 13. September 2021

(Kirchliches Amtsblatt Erzbistum Hamburg, 27. Jg. Nr. 9, Art. 113, S. 196 ff., v. 17. September 2021)

- Amtliche Lesefassung -

Aufgrund § 3 des Gesetzes über die Auftragsdatenverarbeitung zwischen juristischen Personen im Erzbistum Hamburg vom 1. September 2021 wird hiermit nachfolgende Durchführungsverordnung erlassen:

§ 1 Umfang der Datenverarbeitung. Die Auftragsverarbeitung umfasst insbesondere:
a) die Bereitstellung der elektronischen Informations- und Datenverarbeitungssysteme, insbesondere die Ausstattung mit Hard- und Software von Arbeitsplatzcomputern;
b) zentrale IT-Systeme (E-Mailsystem, Dateiablagesysteme, Archivierungssysteme, IT-Sicherheitssysteme, IT-Verwaltungssysteme);
c) Personalverwaltung und -abrechnung, Besoldung, Finanzbuchhaltung, Buchführung;
d) Kassengeschäfte, Spendenverwaltung, Immobilienverwaltung, Friedhofsverwaltung;
e) das kirchliche Meldewesen, Verwaltungsaufgaben für Kirchengemeinden;
f) Verwaltungsaufgaben für Tageseinrichtungen für Kinder, Verwaltungsaufgaben für Büchereien, Verwaltungsaufgaben für Bildungshäuser, Plattformbereitstellung für Onlineschulungen, Datenschutztätigkeiten;
g) Schulungen, Aus-, Fort- und Weiterbildungen oder sonstige entsprechende Veranlassungen.

§ 2 Konkretisierung des Auftragsinhalts. (1) Hiermit wird die Verarbeitung im Hinblick auf Art und Zweck der Aufgaben des Verarbeiters wie folgt näher beschrieben: Bereitstellung, Administration, Betrieb, Durchführung und Betreuung der in § 1 genannten Arten der Verarbeitung zur Sicherstellung der ordnungsgemäßen Verwaltungstätigkeit bei den in § 1 Absatz 1 des Gesetzes über die Auftragsdatenverarbeitung zwischen juristischen Personen im Erzbistum Hamburg genannten juristischen Personen.

(2) Die Verarbeitung findet ausschließlich in einem Mitgliedsstaat 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.

(3) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten und -kategorien:
a) Personenstammdaten, insbesondere Namen, Geburtsdaten, Anschriften;
b) Kommunikationsdaten, insbesondere Telefonkontakte, E-Mail;
c) Vertragsstammdaten, insbesondere Vertragsbeziehung, Vertragsinteresse;
d) Vertragsabrechnungs-, Zahlungs- und Bankdaten;
e) Planungs- und Steuerungsdaten;
f) kirchliche und kommunale Meldedaten nach dem Bundesmeldegesetz;
g) Daten zur Personalverwaltung, insbesondere Sozialversicherungsdaten und Vergütung;
h) Daten für die Verwaltung von Tageseinrichtungen für Kinder;
i) Daten für die Verwaltung von Büchereien;
j) Daten für die Verwaltung von Schulen und pädagogischen Netzen;
k) Daten für die Verwaltung von Bildungshäusern;

l) Daten für die Verwaltung von Beratungsstellen, insbesondere Ehe-, Familien- und Lebensberatung;
m) personenbezogene Vorgangsdaten in Akten.

(4) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
a) Kirchenmitglieder einschließlich deren Familienangehörige;
b) Abonnenten, Lieferanten, Kunden;
c) Dienstnehmer im Sinne des § 4 Ziffer 24 KDG;
d) Vertragsparteien, Nutzungsberechtigte, sonstige Dritte;
e) Ansprechpartner.

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

(2) Der Verarbeiter hat die Sicherheit gemäß § 29 Absatz 4 Buchstabe c, § 26 KDG insbesondere in Verbindung mit § 7 Absatz 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 Absatz 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 das Konzept zur Löschung, das Recht auf Vergessenwerden, die Berichtigung, die Datenportabilität und die Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Verarbeiter sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Verarbeiters. Dem Verarbeiter obliegen neben der Einhaltung der Regelungen dieser Verordnung zudem die gesetzlichen Pflichten gemäß §§ 26, 29 bis 33 KDG; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
a) Die 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 Absatz 5, § 29 Absatz 4 Buchstabe 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 Absatz 4 Buchstabe 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 Verantwortlicher 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 insbesondere als Telekommunikationsleistungen, Post- und 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. 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 zu Beginn der Verarbeitung eine Liste der Unterverarbeiter vor und unterrichtet ihn unverzüglich bei etwaigen Änderungen. Die Unterrichtung muss mindestens in Textform erfolgen.

(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 Europäischen Union oder des Europäischen Wirtschaftsraumes stellt der Verarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Absatz 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterverarbeiter bedarf der ausdrücklichen Zustimmung des Verarbeiters. Die Zustimmung bedarf der 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 Verantwortlicher 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-Sicherheits- oder 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 insbesondere

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 Verantwortlicher 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 in Textform.

(2) Der Verarbeiter hat den Verantwortlichen unverzüglich 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, 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 Natürliche Personen. Soweit in dieser Verordnung auf natürliche Personen Bezug genommen wird, gilt dies – ausgenommen Geistliche – für alle natürlichen Personen gleich welchen Geschlechts.

§ 12 Inkrafttreten. Diese Verordnung tritt mit Wirkung vom 15. September 2021 in Kraft.

Hamburg, den 13. September 2021

L. S.

Ansgar Thim
- Generalvikar -