# Arbeitshilfe mit Erläuterungen zur Vereinbarung über die Verarbeitung von personenbezogenen Daten im Auftrag gemäß § 30 Datenschutzgesetz-EKD (DSG-EKD)

# Inhalt

# Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 30 EKD-Datenschutzgesetz (DSG-EKD)

zwischen

**Bezeichnung der verantwortlichen Stelle**

Straße Hausnummer

Postleitzahl Ort

(nachfolgend bezeichnet als „Auftraggeber“)

und

**Bezeichnung des Auftragsverarbeiters**

Straße Hausnummer

Postleitzahl Ort

(nachfolgend bezeichnet als „Auftragsverarbeiter“)

## Begriffsbestimmungen

**„Hauptvertrag“** bezeichnet den zwischen den Parteien am [Datum] geschlossenen [Dienstvertrag/Werkvertrag].

**„Daten“** bezeichnet personenbezogene Daten im Sinne des § 4 Nummer 1 DSG-EKD.

**„Auftragsverarbeitung“** (kurz: **„AV“**) bezeichnet die Verarbeitung von Daten durch den Auftragsverarbeiter im Auftrag des Auftraggebers.

**„AVV“** bezeichnet den vorliegenden Vertrag zur Regelung der Auftragsverarbeitung. Paragraphen ohne Gesetzesangabe bezeichnen solche des AVV.

## Präambel

Der Hauptvertrag umfasst Leistungen der Auftragsverarbeitung. Entsprechend den gesetzlichen Vorgaben des § 30 DSG-EKD konkretisiert die vorliegende Vereinbarung die datenschutzrechtlichen Verpflichtungen der Parteien bei Durchführung der Auftragsverarbeitung.

Ziel des vorliegenden Vertrags ist die datenschutzkonforme Durchführung jeglicher aufgrund des Hauptvertrags stattfindender Datenverarbeitung. Dies betrifft sowohl die Verarbeitung von Daten, welche der Auftraggeber an den Auftragsverarbeiter übergibt, als auch Daten, die im Auftrag des Auftraggebers erstmalig durch den Auftragsverarbeiter erhoben werden. Dieser Vertrag gilt für alle Tätigkeiten und Anwendungen, bei denen Mitarbeitende des Auftragsverarbeiters oder – soweit der Auftraggeber eine Unterbeauftragung zugelassen hat – durch den Auftragsverarbeiter beauftragte Dritte mit diesen Daten in Berührung kommen können. Für rechtliche hier nicht näher definierte Begriffe oder Ausdrücke gelten die maßgeblichen gesetzlichen Definitionen des DSG-EKD.

## § 1
## Gegenstand und Dauer des Auftrags

(1) Gegenstand des Hauptvertrags ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter für den Auftraggeber nach dessen Weisung:

[Definition der Aufgaben]

(2) Diese Vereinbarung gilt ab dem 24.05.2018 und endet nach der Beendigung des Hauptvertrages mit der Übergabe oder der Vernichtung aller personenbezogenen Daten des Auftraggebers gemäß § 10 dieser Vereinbarung, ohne dass es einer gesonderten Kündigung dieser Vereinbarung bedarf.

## § 2
## Konkretisierung des Auftragsinhalts

(1) Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle gemäß § 30 Absatz 1 Satz 1 DSG-EKD.

(2) Der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten, die Art der Daten und der Kreis der betroffenen Personen werden wie folgt festgelegt:

1. Art der Daten

Gegenstand der Verarbeitung von Daten (dazu gehören auch neu entstehende Daten) durch den Auftragsverarbeiter sind folgende Datenarten bzw. -kategorien:

[Aufzählung, Beschreibung der Datenkategorien, z. B. Personenstammdaten, Kommunikationsdaten wie etwa Telefonnummern, E-Mail-Adressen, Vertragsstammdaten wie etwa Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten, Beispiel Buchhaltung: Rechnungsdaten, Lieferantendaten, Debitoren und Kreditoren, Adressdaten, Bankverbindungen, Gläubiger-ID nach SEPA, Ansprechpartner bei Lieferanten, Telefonnummern, Steuernummern]

2. Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten

Umfang, Art und Zweck der Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter für den Auftraggeber sind in den folgenden Dokumenten näher beschrieben:

[Benennung/Aufzählung der relevanten Dokumente und des einschlägigen Textabschnitts sowie Verweis auf entsprechende Anlage zu diesem Vertrag]

bzw. werden wie folgt näher beschrieben:

[Umfassende Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Datenverarbeitung durch den Auftragsverarbeiter; bzgl. der Art der Verarbeitung kommen insbeseondere in Betracht: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten]

3. Kreis der betroffenen Personen

Der Kreis der im Rahmen dieses Auftrags durch den Umgang mit ihren personenbezogenen Daten betroffenen Personen umfasst [Aufzählung/Beschreibung der betroffenen Personenkategorien, z. B. Gemeindeglieder, Patienten, Mitarbeitende, Abonnenten, Lieferanten, Pächter, Mieter, Ansprechpersonen].

## § 3
## Technische und organisatorische Maßnahmen

(1) Die Verarbeitung von Daten durch den Auftragsverarbeiter findet nur auf Datenverarbeitungsanlagen statt, für die zum Schutz der Daten technische und organisatorische Maßnahmen gemäß § 27 DSG-EKD getroffen wurden. Der Auftragsverarbeiter verpflichtet sich, in seinem betrieblichen Verantwortungsbereich alle technischen und organisatorischen Maßnahmen zu treffen, die nach § 27 DSG-EKD zur Durchführung des in § 1 beschriebenen Auftrages notwendig sind. Hierzu zählen insbesondere die in Anlage 1 dieses Vertrags beschriebenen Maßnahmen. Sie definieren die vom Auftragsverarbeiter einzuhaltenden Minimalanforderungen.

Soweit im Hauptvertrag keine abweichende Vereinbarung getroffen wurde, trägt der Auftragsverarbeiter die mit den technischen und organisatorischen Maßnahmen verbundenen Kosten.

Der Auftragsverarbeiter stellt dem Auftraggeber sein jeweils aktuelles IT-Sicherheitskonzept zur Verfügung.

(2) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragsverarbeiter den Auftraggeber unverzüglich.

Der Auftragsverarbeiter ist berechtigt, die technischen und organisatorischen Maßnahmen der technischen und organisatorischen Weiterentwicklung entsprechend anzupassen, soweit es sich nicht um wesentliche Anpassungen handelt und das im AVV vereinbarte Sicherheitsniveau nicht unterschritten und die Anforderungen des § 27 DSG-EKD erfüllt werden. Zur Aufrechterhaltung des bestehenden Sicherheitsniveaus erforderliche Anpassungen hat der Auftragsverarbeiter unverzüglich umzusetzen.

Wesentliche Anpassungen der technischen und organisatorischen Maßnahmen sind zwischen den Parteien zu vereinbaren. Zu diesem Zweck wird der Auftragsverarbeiter dem Auftraggeber unverzüglich benachrichtigen, soweit er beabsichtigt wesentliche Anpassungen vornehmen.

(3) Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber alle von ihm getroffenen technischen und organisatorischen Maßnahmen unaufgefordert in Form einer aktualisierten Fassung der Anlage 1 zur Kenntnis zu bringen, soweit sie von dieser Vereinbarung abweichen. Der Auftraggeber trägt die Verantwortung dafür, dass die vom Auftragsverarbeiter getroffenen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(4) Verarbeitet der Auftragsverarbeiter auch andere Daten als solche des Auftraggebers, garantiert der Auftragsverarbeiter, dass diese Daten durch technische und organisatorische Maßnahmen von den Daten des Auftraggebers getrennt sind und bleiben.

(5) Soweit der Auftragsverarbeiter zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gesetzlich verpflichtet ist, hat er dieses dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

## § 4
## Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(2) Auskünfte an Dritte und an betroffene Personen darf der Auftragsverarbeiter nur nach vorheriger Zustimmung seitens des Auftraggebers erteilen.

Soweit eine betroffene Person sich zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer Daten oder zwecks Auskunft unmittelbar an den Auftragsverarbeiter wenden sollte, wird der Auftragsverarbeiter die betroffene Person an den Auftraggeber verweisen. Der Auftragsverarbeiter wird das Ersuchen der betroffenen Person unverzüglich an den Auftraggeber weiterleiten.

(3) Ist der Auftraggeber gegenüber einer betroffenen Person verpflichtet, dieser Auskünfte zur Auftragsverarbeitung zu erteilen, wird der Auftragsverarbeiter auf eigene Kosten den Auftraggeber bei der Ermittlung der zu diesem Zweck benötigten Informationen unterstützen.

## § 5
## Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter stellt sicher, dass bei Durchführung der nach § 1 in seinem Verantwortungsbereich durchzuführenden Tätigkeiten das DSG-EKD sowie sämtliche speziellen datenschutzrechtlichen Vorschriften, denen der Auftraggeber unterliegt, eingehalten werden.

Er verpflichtet sich, das Datengeheimnis zu wahren und für die Datenverarbeitung nur solche Beschäftigten oder sonstigen Personen einzusetzen, die auf das Datengeheimnis verpflichtet worden sind. Die Verpflichtung von Beschäftigten oder sonstigen Personen auf das Datengeheimnis hat unter Hinweis auf die möglichen Folgen des Verstoßes gegen datenschutzrechtliche Pflichten zu erfolgen. Auf Verlangen des Auftraggebers wird der Auftragsverarbeiter die Verpflichtung der Beschäftigten und sonstigen Personen nachweisen.

Der Auftragsverarbeiter überwacht fortlaufend die Einhaltung datenschutzrechtlicher Vorschriften durch die eingesetzten Beschäftigten und sonstigen Personen.

(2) Der Auftragsverarbeiter verwendet die Daten für keine anderen als die im AVV festgelegten Zwecke. Der Auftragsverarbeiter verpflichtet sich, dass die Inhalte, die ihm anlässlich der Auftragsverarbeitung zur Kenntnis gelangt sind, sowie die Arbeitsergebnisse keinem Unbefugten zur Kenntnis gelangen. Diese Verpflichtung besteht auch nach Beendigung des Vertrags fort. Kopien und Duplikate werden nur mit Zustimmung des Auftraggebers erstellt. Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten durch den Auftragsverarbeiter erforderlich sind, dürfen erstellt werden.

(3) Der Auftragsverarbeiter ist verpflichtet, Kontrollen durch regelmäßige Prüfungen im Hinblick auf die Vertragsausführung bzw. Vertragserfüllung durchzuführen. Dazu gehört auch die Kontrolle technischer und organisatorischer Maßnahmen nach § 3 dieses Vertrages. Dem Auftraggeber sind die Prüfprotokolle auf Verlangen unverzüglich vorzulegen.

(4) Der nicht-kirchliche Auftragsverarbeiter unterstellt sich der Kontrolle der zuständigen kirchlichen Datenschutzaufsichtsbehörde. Diese Behörde nimmt insbesondere die Aufgaben nach § 43 DSG-EKD sowie die Befugnisse nach § 44 DSG-EKD unmittelbar gegenüber dem nichtkirchlichen Auftragsverarbeiter wahr.

(5) Der Auftragsverarbeiter wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den §§ 27, 32, 33 und 34 DSG-EKD, genannten Pflichten unterstützen.

Der Auftragsverarbeiter wird den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, ihren Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 des DSG-EKD geregelten Rechte der betroffenen Person nachzukommen.

(6) Dem Auftraggeber steht für den Fall der Verlagerung der Datenverarbeitung in ein Drittland gemäß § 10 DSG-EKD ein außerordentliches Kündigungsrecht zu.

Der Auftragsverarbeiter hat die konkreten Orte der Leistungserbringung stets aktuell zu dokumentieren und auf Verlangen dem Auftraggeber nachzuweisen.

(7) Die Auftraggeber kann jederzeit während des Bestehens des Vertragsverhältnisses schriftlich sämtliche im Rahmen der AV verarbeiteten Daten herausverlangen. Soweit die Daten auf

einem Speichermedium herausgegeben werden, ist der Schutz der Daten durch technische und organisatorische Maßnahmen sicherzustellen.

(8) Die Verarbeitung von Daten in Privatwohnungen ist grundsätzlich nicht zulässig. Ausnahmen bedürfen der vorherigen schriftlichen Zustimmung durch den Auftraggeber. Für den jeweiligen Einzelfall sind die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten festzulegen. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber oder die Beauftragte für den Datenschutz der EKD oder den Beauftragten für den Datenschutz der EKD vorher mit dem Auftragsverarbeiter abzustimmen. Der Auftragsverarbeiter sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(9) Der Auftragsverarbeiter bestätigt, dass er einen fachkundigen und zuverlässigen örtlich Beauftragten für den Datenschutz bestellt hat und verpflichtet sich, die Bestellung eines örtlich Beauftragten für den Datenschutz während der Dauer des Vertrages aufrechtzuhalten, auch wenn die gesetzlichen Voraussetzungen für eine Bestellpflicht entfallen sollten. Die Kontaktdaten des örtlich Beauftragten für den Datenschutz ergeben sich aus der Anlage 2. Einen Wechsel in der Person des örtlich Beauftragten für den Datenschutz hat der Auftragsverarbeiter dem Auftraggeber unverzüglich schriftlich mitzuteilen.

## § 6
## Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter erbringt die nachfolgend aufgeführten Leistungen ausschließlich durch folgende Unterauftragnehmer.

[Art der Leistung, Name und Kontaktdaten]

(2) Die Verträge des Auftragsverarbeiters mit seinen Unterauftragnehmern sind derart gestaltet, dass sie den Anforderungen der gemäß § 5 Absatz 1 jeweils anwendbaren gesetzlichen Bestimmungen über den Datenschutz genügen und dass die Unterauftragnehmer unmittelbar gegenüber dem Auftraggeber dieselben Verpflichtungen übernehmen, die dem Auftragsverarbeiter gemäß dem AVV obliegen.

Der Auftragsverarbeiter haftet für das Handeln von Unterauftragnehmern wie für eigenes Handeln. Die Verträge sind auf Verlangen des Auftraggebers in Kopie zu übergeben. Die mit den Unterauftragnehmern ausgehandelten Preise können geschwärzt werden.

(3) Die Durchführung weiterer Unterbeauftragungen sowie der Abschluss entsprechender Verträge über die Erbringung der in § 6 Absatz 1 bestimmten Leistungen mit den aufgezählten oder anderen Unterauftragnehmern bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Holt der Auftragsverarbeiter im Falle einer weiteren Unterbeauftragung entgegen § 6 Absatz 3 Satz 1 die vorherige Zustimmung des Auftraggebers nicht ein, berechtigt dies den Auftraggeber zur außerordentlichen Kündigung des Vertrags mit dem Auftragsverarbeiter.

(4) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungspersonal, Wirtschaftsprüfung oder die Entsorgung von Datenträgern. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleis-

tungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

## § 7
## Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die nach § 30 Absatz 3 Satz 3 vorgesehene Überprüfung durchzuführen oder durch im Einzelfall zu benennende Personen durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung ihrer Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

(2) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 30 Absatz 3 Satz 3 DSG-EKD und im Wege der Datenschutz-Folgenabschätzung nach § 34 DSG-EKD stellt der Auftragsverarbeiter sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter den Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 27 Absatz 1 DSG-EKD und der Anlage 1 dieses Vertrages nach. Die Einhaltung von genehmigten Verfahrensregeln und die Verwendung zertifizierter und kirchlich geprüfter Informationstechnik können gemäß § 30 Absatz 8 DSG-EKD herangezogen werden, um die Erfüllung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter nachzuweisen. Auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfung, Revision, Compliance-Beauftragte(r), Datenschutzbeauftragte(r), IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit, z. B. nach BSI-Grundschutz) kann der Nachweis erbracht werden.

(3) Die Prüfungs-, Zutritts- und Auskunftsrechte stehen auch der oder dem Beauftragten für den Datenschutz der Evangelisch-Lutherischen Kirche in Norddeutschland zu.

## § 8
## Informations- und Unterstützungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter wird den Auftraggeber benachrichtigen, wenn ihm Verletzungen des Schutzes personenbezogener Daten durch den Auftragsverarbeiter, seine Unterauftragnehmer oder die beim Auftragsverarbeiter oder seinen Unterauftragnehmern beschäftigten Personen oder ein entsprechender Verdacht bekannt werden. Die Benachrichtigungspflicht des Auftragsverarbeiters besteht auch bei schwerwiegenden Betriebsstörungen, bei Verstößen gegen die im AVV getroffenen Festlegungen (dazu gehören auch vertragsrelevante technische oder organisatorische Störungen) oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten im Auftrag des Auftraggebers. Die Benachrichtigung hat unverzüglich zu erfolgen.

Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese der verantwortlichen Stelle unverzüglich. Der Auftragsverarbeiter unterstützt die kirchliche Stelle kostenfrei bei der Benachrichtigung der betroffenen Personen.

Der Auftragsverarbeiter hat in diesen Fällen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für betroffene Personen zu ergreifen. Der Auftraggeber ist über die getroffenen Maßnahmen zu informieren.

(2) Über Maßnahmen von Strafverfolgungsorganen wird der Auftragsverarbeiter den Auftraggeber unaufgefordert und unverzüglich benachrichtigen, soweit hierdurch die Datenverarbeitung für den Auftraggeber betroffen ist oder sein kann. Die Benachrichtigungspflicht des Auftraggebers besteht nicht, soweit dieser durch die Benachrichtigung gegen ein gesetzliches Verbot verstoßen würde.

(3) Über Kontrollen und Maßnahmen der oder des staatlichen Datenschutzbeauftragten oder der oder des Beauftragten für den Datenschutz der Evangelisch-Lutherischen Kirche in Norddeutschland wird der Auftragsverarbeiter den Auftraggeber unaufgefordert unverzüglich in Kenntnis setzen, sofern hierdurch die Datenverarbeitung für den Auftraggeber betroffen ist.

## § 9
## Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der gemäß dem AVV durchgeführten Auftragsverarbeitung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das sie durch Einzelweisungen konkretisieren kann. Der Auftragsverarbeiter wird die Weisungen des Auftraggebers beachten und befolgen und sie einer angemessenen Nachkontrolle auf Richtigkeit und Plausibilität unterziehen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in Textform (§ 126b BGB) bestätigen.

(3) Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften oder gegen den AVV. Der Auftragsverarbeiter ist berechtigt, die Durchführung einer Weisung, die seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstößt, so lange auszusetzen, bis diese durch den Weisungsberechtigten beim Auftraggeber bestätigt oder geändert wird. Über seine Bedenken hat er den Auftraggeber unverzüglich und in begründeter Form zu informieren.

(4) Zur Erteilung und zum Empfang von Weisungen betreffend die Auftragsverarbeitung sind ausschließlich die in Anlage 2 genannten Personen berechtigt. Jede Partei ist berechtigt, die Benennung berechtigter Personen jederzeit durch schriftlich Mitteilung gegenüber der jeweils anderen Partei mit einer Ankündigungsfrist von zwei Wochen zu ändern. Bei einem Wechsel oder einer dauerhaften Verhinderung einer benannten Person ist dies der anderen Partei unverzüglich schriftlich unter Benennung eines Vertreters mitzuteilen.

## § 10
## Löschung von Daten und Rückgabe von Datenträgern, Dokumentation

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber, spätestens jedoch mit der Beendigung des Hauptvertrages hat der Auftragsverarbei-

ter sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Vervielfältigungen der Daten des Auftraggebers (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragsverarbeiters sowie für Test- und Ausschussmaterial. Das zur Datenlöschung anzuwendende Löschverfahren wird in der Anlage 1 näher beschrieben. Die Löschung der Daten ist zu protokollieren, und das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragsverarbeiter entsprechend den jeweiligen gesetzlichen oder zwischen den Parteien vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## § 11
## Formklausel

Änderungen und Ergänzungen des AVV, der mit Bezug hierauf zwischen den Parteien getroffenen weiteren Vereinbarungen sowie alle unmittelbar den Inhalt oder den Umfang der von den Parteien unter diesem AVV geschuldeten Leistungen ändernden oder sonst beeinflussenden Erklärungen bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Abänderung dieser Schriftformklausel.

## § 12
## Salvatorische Klausel mit Ersetzungsklausel

Sollte eine der Regelungen des AVV oder einer mit Bezug hierauf geschlossenen weiteren Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden oder der AVV eine nach übereinstimmender Auffassung der Parteien regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Regelungen nicht. Anstelle der unwirksamen Regelung oder in Ausfüllung der Lücke gelten die gesetzlichen Bestimmungen.

| Bezeichnung des Auftraggebers | Bezeichnung des Auftragsverarbeiters |
|---|---|
| _____ | _____ |
| (Ort, Datum) | (Ort, Datum) |
| _____ | _____ |
| (Unterschriften mit Amts- / Funktionsbezeichnungen) | (Unterschriften mit Amts- / Funktionsbezeichnungen) |

Anlagen: 2

# Anlage 1: Technische und organisatorische Maßnahmen und IT-Sicherheit

Unbeschadet der aus § 27 DSG-EKD resultierenden Pflichten des Auftragnehmers definieren die nachfolgenden Bestimmungen die Mindestanforderungen an die technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Gewährleistung von Datenschutz und Datensicherheit zu treffen und laufend aufrecht zu erhalten hat. Insbesondere hat der Auftragnehmer die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen sicherzustellen.

[Die Maßnahmen sind so konkret, präzise und detailliert wie möglich zu beschreiben, da diese Anlage im Rahmen der Durchführung der AV als Maßstab sowohl für Umfang und Reichweite der Pflichten des Auftragsverarbeiters, als auch für die Kontrollen des Auftraggebers herangezogen wird. Für einen sachkundigen Dritten muss allein aufgrund der Beschreibung zweifelsfrei erkennbar ist, wie die vom Auftragsverarbeiter zu erfüllenden Minimalanforderungen definiert sind. Eine Verweisung auf separate Quellen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist daher ausgeschlossen.]

# Anlage 2: Berechtigte Weisungsgeber und Weisungsempfänger, Datenschutzbeauftragte

Zur Erteilung von Weisungen betreffend die Auftragsverarbeitung sind aufseiten des Auftraggebers folgende Personen[1] berechtigt:

25T
(Name, Funktion, Anschrift, Telefon, Fax, E-Mail)

Zum Empfang von Weisungen betreffend die Auftragsverarbeitung sind aufseiten des Auftragsverarbeiters ausschließlich folgende Personen berechtigt:

25T
(Name, Funktion, Anschrift, Telefon, Fax, E-Mail)

Beim Auftragsverarbeiter ist folgende Person

[Name und Kontaktdaten]

☐ als örtlich Beauftragte(r) für den Datenschutz bestellt.

☐ als Beauftragte(r) für den Datenschutz bestellt
(siehe Art. 37 EU-Datenschutz-Grundverordnung, § 38 Bundesdatenschutzgesetz).

Beim Auftraggeber ist folgende Person

[Name und Kontaktdaten]

als örtlich Beauftragte(r) für den Datenschutz bestellt.

[1] ggf. auch die oder den örtlich Beauftragte(n) für den Datenschutz als weisungsberechtigte Person aufnehmen.

# Erläuterungen / Ausfüllhinweise zur Arbeitshilfe zur Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 30 Datenschutzgesetz-EKD

Die Auftragsverarbeitung muss unter Beachtung und Umsetzung der für den Auftraggeber geltenden Vorschriften abgewickelt werden (Datenschutzgesetz-EKD, Datenschutzdurchführungsverordnungen der EKD und der Gliedkirchen u. a.). Bei einer Auftragsverarbeitung ist nicht der Auftragsverarbeiter für die Einhaltung der kirchlichen Datenschutzvorschriften verantwortlich. Da der Auftragsverarbeiter datenschutzrechtlich wie eine organisatorische Einheit des Auftraggebers und nicht als Dritter behandelt wird, verbleibt auch die Verantwortlichkeit beim Auftraggeber. Sie ist insb. verpflichtet, den Auftragsverarbeiter sorgfältig auszuwählen und sich durch Kontrollen von der Einhaltung der Datenschutzvorschriften durch den Auftragsverarbeiter zu überzeugen. Der Auftragsverarbeiter muss seinerseits intern sicherstellen, dass die Datenerhebung, -verarbeitung und -nutzung nur nach den durch den Auftraggeber festgelegten Weisungen erfolgt und die notwendigen technischen und organisatorischen Maßnahmen zu treffen.

## Zur Präambel

Die Angaben in der Präambel sind vor allem für die Auslegung der weiteren Regelungen des AVV relevant.

Beim Hauptvertrag handelt es sich in der Regel um einen Dienst- oder Werkvertrag, der insb. die vom Auftragsverarbeiter zu erbringenden Leistungen festlegt. Darüber hinaus können – je nach Einzelfall – z. B. Regelungen zu den Themen Vergütung, Laufzeit, Kündigung, Schadenersatz, Vertragsstrafe, Haftung, anwendbares Recht und Gerichtsstand aufgenommen werden. In der Vergütungsregelung des Hauptvertrags sollte insbesondere bestimmt werden, dass die Kosten für das Datenschutz- und IT-Sicherheitskonzept vom Auftragsverarbeiter zu tragen sind. Der Hauptvertrag und die in ihm enthaltene Leistungsbeschreibung stellen die Grundlage für die Weisungen des Auftraggebers dar.

Der Auftraggeber hat als „Herrin der Daten“ bereits bei Auftragserteilung durch den AVV zu regeln, wie die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter erfolgen soll, wie dies organisatorisch abläuft, welche Datensicherheitsmaßnahmen erforderlich sind und wie einzelne Vorgaben technisch umgesetzt werden sollen. Bereits bei der Auswahl eines geeigneten Auftragsverarbeiters ist auf die Einhaltung der Vorgaben zu achten. In der Praxis werden viele dieser Anforderungen Vorgaben bereits umgesetzt sein. Kann ein potenzieller Auftragsverarbeiter diese Vorgaben nicht umsetzen, kommt er für die Durchführung einer Auftragsverarbeitung im Sinne des § 30 DSG-EKD nicht in Betracht.

## Zu § 1 Absatz 1 und 2

Siehe auch § 30 Absatz 3 Satz 2 Nummer 1 DSG-EKD. Soweit Gegenstand und Dauer der Auftragsverarbeitung mit denen des jeweiligen Hauptvertrags identisch sind, kann unter § 1 Absatz 1 auf die relevante Stelle im Hauptvertrag verwiesen werden (z. B. „Der Gegenstand des Auftrags ergibt sich aus § 2 Absatz 1 bis 3 des Hauptvertrags“). Der Verweis sollte zur eindeutigen Bestimmung der Vertragsinhalte so konkret wie möglich gestaltet und der Hauptvertrag als Anhang zum vorliegenden AVV geführt werden.

Bedeutsam für den AVV ist vor allem die Laufzeitregelung des Hauptvertrags da § 1 Absatz 2 auf diese verweist.

Auch für Aufträge, welche die (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen betreffen, muss nach § 30 Absatz 6 DSG-EKD ein AVV abgeschlossen werden, wenn bei Durchführung des Auftrags ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. In der Praxis kann es bei vielen Dienstleistungen der IT-Branche zu einer ggf. unbeabsichtigten Kenntnisnahme personenbezogener Daten durch den Auftragsverarbeiter kommen. Hierbei ist etwa an die Installation und Wartung von Netzwerken und Hardware (incl. Telekommunikationsanlagen) sowie die Pflege von Software (z. B. Betriebssysteme, Anwendungen), Programmentwicklungen, Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests, Durchführung von Migrationen im Produktivsystem und das Parametrisieren von Software zu denken.

Bei der entsprechenden Anwendung von § 30 Absatz 1 bis 5 DSG-EKD sind etwaige Besonderheiten, die für die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen charakteristisch sind, zu berücksichtigen. Dabei ist es unerheblich, ob die Wartungsmaßnahmen vor Ort oder per Fernwartung als Remote-Zugriff des Auftragsverarbeiters auf personenbezogene Daten bei dem Auftraggeber durchgeführt werden.

## Zu § 2 Absatz 2

Siehe auch § 30 Absatz 3 Satz 2 Nummer 2 DSG-EKD. Die Festlegungen haben unmittelbare Auswirkungen auf die Rechtmäßigkeit des Datenumgangs durch den Auftragsverarbeiter. Sie sollen eindeutig und vollständig aufgeführt werden.

Soweit zur Bestimmung von Umfang, Art und Zweck der Datenverarbeitung auf separate Dokumente verwiesen wird, sollten die einschlägigen Textabschnitte möglichst genau benannt werden, z. B. durch Verweis auf konkrete Paragraphen des Hauptvertrags. Darüber hinaus sollten sie jeweiligen Dokumente als Anlage zum AVV geführt werden.

## Zu § 3

Nach § 30 Absatz 3 Satz 2 Nummer 3 DSG-EKD sind zwingend Angaben zu den vereinbarten technischen und organisatorischen Maßnahmen nach § 27 DSG-EKD in den AVV aufzunehmen. Zur Umsetzung dieser Pflicht ist insbesondere der gesamte Ablauf vom Transport der Daten über die Festlegung der Zugriffsrechte bis zur Löschung der Daten in der gesonderten Anlage 1 darzustellen. In vielen Fällen können hierbei bereits bestehende Datenschutz- und IT-Sicherheitskonzepte Orientierungszwecken herangezogen werden. Die schriftliche Fixierung hilft dem Auftraggeber, zum einen bei effektiven der Wahrnehmung ihrer Kontrollrechte gegenüber dem Auftragsverarbeiter. Zum anderen kann sie vom Auftraggeber herangezogen werden, um ihrer Nachweispflicht aus § 5 Absatz 2 DSG-EKD nachzukommen.

## Zu § 3 Absatz 1 Satz 5

Bei der Verarbeitung personenbezogener Daten ist vom Auftraggeber der Schutzbedarf festzulegen. Bei einem mittleren oder hohen Schutzbedarf der personenbezogenen Daten ist ein IT-Sicherheitskonzept vorzulegen. In anderen Fällen, insbesondere wenn der Schutzbedarf der personenbezogenen Daten als einfach eingestuft ist, kann im Einzelfall von der Übergabe des IT-Sicherheitskonzeptes abgesehen werden. In diesen Fällen kann Absatz 1 Satz 5 der Vereinbarung gestrichen werden. Dabei wird vorausgesetzt, dass angemessene Schutzmaßnahmen nach der Anlage 1 dieser Vereinbarung realisiert sind.

## Zu § 3 Absatz 5

Die logische Datentrennung von Daten Dritter ist auch zwingender Bestandteil der Anlage 1. Zulässige Maßnahmen können z. B. softwareseitiger Ausschluss (Mandantentrennung), Datei-

separierung bei Datenbankprinzip, Trennung über Zugriffsregelung, Trennung von Test- und Routineprogrammen sein.

## Zu § 4

Siehe auch § 30 Absatz 3 Satz 2 Nummer 4 DSG-EKD.

## Zu § 4 Absatz 1

Hinsichtlich der Löschung von Daten kann es erforderlich sein, Löschfristen und die Verfahrensabläufe bei der Löschung detailliert festzulegen. Alternativ kann auch die folgende Formulierung verwendet werden:

*„(1) Wird festgestellt, dass Daten unrichtig sind, hat sie der Auftragsverarbeiter nach Abstimmung mit dem Auftraggeber unverzüglich zu berichtigen. Die Verarbeitung von für das laufende Verfahren nicht mehr benötigten Daten ist einzuschränken. Gesetzliche Aufbewahrungs- oder Archivierungspflichten sind zu beachten, anderenfalls sind sie zu löschen."*

## Zu § 4 Absatz 2

Bei der Auftragsverarbeitung bleibt der Auftraggeber Adressat der Ansprüche von betroffenen Personen, die ihre Rechte auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung geltend machen können.

## Zu § 5 Absatz 1 Satz 2

Die Verpflichtung der Mitarbeitenden auf das Datengeheimnis ist zwingend, sofern der Auftragsverarbeiter eine nichtkirchliche Stelle (in der Regel aus der Privatwirtschaft) ist. Bei beauftragten kirchlichen Stellen entfällt die Verpflichtung nach § 26 Satz 2 DSG-EKD, wenn die Mitarbeitenden des Auftragsverarbeiters auf Grund anderer kirchlicher arbeits- oder beamtenrechtlicher Bestimmungen zur Verschwiegenheit verpflichtet sind. Für die Verpflichtung der Beschäftigten des Auftragsverarbeiters ist das Formblatt nach den jeweiligen Durchführungsbestimmungen zu verwenden.

## Zu § 5 Absatz 4

Siehe auch § 11 Absatz 5 DSG-EKD. Dieser Absatz kann entfallen, sofern es sich bei dem Auftragsverarbeiter um eine kirchliche Stelle handelt.

## Zu § 5 Absatz 6

Nachdem mit dem Inkrafttreten der EU-Datenschutz-Grundverordnung in der gesamten Europäischen Union ein einheitlich hohes Datenschutzniveau etabliert wurde, stellt das DSG-EKD an die Auftragsverarbeitung in anderen EU-Mitgliedstaaten dieselben Anforderungen wie an die Auftragsverarbeitung innerhalb Deutschlands. Darüber hinaus ist unter den Voraussetzungen des § 10 DSG-EKD in Verbindung mit § 30 Absatz 2 DSG-EKD auch eine Auftragsverarbeitung außerhalb der Europäischen Union möglich. Jedoch ist für den Fall der Datenverarbeitung in einem anderen EU-Mitgliedsstaat zu berücksichtigen, dass grenzüberschreitende Auftragsverarbeitungen in die vom Auftraggeber regelmäßig durchzuführenden Datenschutzkontrollen einzubeziehen sind. Mit Blick auf Kontrollen am Dienstsitz des Auftragsverarbeiters können dem Auftraggeber daher im Vergleich zur Auftragsverarbeitung innerhalb Deutschlands erhebliche organisatorische und wirtschaftliche Mehraufwände entstehen. Soll die Auftragsdatenverarbeitung außerhalb Deutschlands stattfinden, ist dies in § 5 Absatz 6 Satz 1 zu konkretisieren.

Der Auftraggeber kann es zulassen, dass der Auftragsverarbeiter seinen Kontrollpflichten auch auf andere Wiese nachkommt (z. B. durch Einschaltung von sachverständigen Dritten, Fragebögen oder Anforderung von Prüfdokumentationen oder Zertifikaten).

## Zu § 5 Absatz 7

Näheres ist in der Anlage 1 zu regeln. In der Regel sollen die Daten verschlüsselt werden.

## Zu § 5 Absatz 8

In dem jeweiligen Ausnahmefall sollte sich der Auftraggeber die zwischen dem Auftragsverarbeiter und seinem Beschäftigten abgeschlossene Vereinbarung vorlegen lassen. Im Rahmen der Überprüfung sind der Arbeitsplatz des Beschäftigten und die festgelegten technischen und organisatorischen Maßnahmen einzubeziehen.

## Zu § 6

Für einzelne Tätigkeitsbereiche der Datenverarbeitung kann es notwendig sein, Unterauftragnehmer einzusetzen. Zwischen dem Auftraggeber und dem Auftragsverarbeiter ist daher die Zulässigkeit oder Nichtzulässigkeit bestehender und zukünftiger Unterauftragsverhältnisse zu regeln.

## Zu § 6 Absatz 3

Hierzu zählen alle Vertragsänderungen. Es kann vereinbart werden, dass Vertragsänderungen ausgenommen sind, die sich ausschließlich in der Vereinbarung neuer Preise erschöpfen.

## Zu § 7

Die kirchliche Stelle bleibt gegenüber den betroffenen Personen nach außen verantwortlich für die Zulässigkeit der Datenverarbeitung. Um das Haftungsrisiko gegenüber den betroffenen Personen zu minimieren, muss der Auftraggeber sich jederzeit, auch nach Beginn der Datenverarbeitung, von der ordnungsgemäßen Vertragsdurchführung durch den Auftragsverarbeiter überzeugen zu können. Es ist nicht in jedem Fall erforderlich, dass sich der Auftraggeber hiervon unmittelbar beim Auftragsverarbeiter vor Ort oder selbst in Person überzeugt. Je nach Einzelfall kann der Nachweis auch anderweitig erbracht werden (siehe § 7 Absatz 2).

## Zu § 7 Absatz 1

Für den Auftraggeber können entsprechend qualifizierte Personen tätig werden (z. B. die oder der örtlich Beauftragte für den Datenschutz). Diese Person nimmt beim Auftragsverarbeiter die Erstkontrolle und die regelmäßigen Kontrollen vor.

## Zu § 7 Absatz 2

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig (z. B. im Rhythmus von ein oder zwei Jahren, in Fällen besonderen Anlasses auch häufiger) von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren. Im Rahmen der Kontrolle sind die in der Anlage aufgeführten Maßnahmen zu begutachten. Bei nichtkirchlichen Stellen gehört zur Überprüfung z. B. auch das Vorlegen der Verpflichtungserklärungen der Mitarbeitenden des Auftragsverarbeiters auf das Datengeheimnis. Die Kontrolle hat sich auch auf Unterauftragnehmer zu erstrecken. Die Überprüfung kann vor Ort erfolgen, oder es können auch die von Dritten durchgeführten Begutachtungen akzeptiert werden, soweit entsprechende Nachweise vorliegen. Bei kirchlichen Stellen als Auftragsverarbeiter sind im Einzelfall die Absätze 2 und 3 entbehrlich.

## Zu § 8

Siehe auch § 30 Absatz 3 Satz 2 Nummer 8 DSG-EKD. Da die kirchliche Stelle gegenüber der betroffenen Person nach außen verantwortlich für die Zulässigkeit der Datenverarbeitung bleibt, muss sie über alle Fehlhandlungen, Störungen oder Unregelmäßigkeiten informiert werden.

Zudem treffen den Auftraggeber und den Auftragsverarbeiter die Meldepflicht aus §§ 32 DSG-EKD. Die dem Auftragsverarbeiter gemäß § 8 aufzuerlegenden Pflichten dürfen keinesfalls hinter den in § 32 Absatz 2 DSG-EKD gesetzlichen Pflichten des Auftragsverarbeiters zurückbleiben. Der Auftraggeber trifft außerdem die Benachrichtigungspflicht aus § 33 DSG-EKD.

## Zu § 8 Absatz 2

Der Klammertext ist nur aufzunehmen, sofern der Auftragsverarbeiter als nichtkirchliche Stelle nicht dem DSG-EKD sondern dem staatlichen Datenschutzrecht (EU-Datenschutz-Grundverordnung bzw. Bundesdatenschutzgesetz) unterliegt.

## Zu § 8 Absatz 3

Bei einer kirchlichen Stelle nach § 1 Absatz 2 DSG-EKD kann der Hinweis auf den „staatlichen Datenschutzbeauftragten“ entfallen.

## Zu § 9

Siehe auch § 30 Absatz 3 Satz 2 Nummer 9 DSG-EKD und § 30 Absatz 4 Satz 1 DSG-EKD. Die Weisungsgebundenheit ist wesentliches Merkmal der Auftragsverarbeitung. Weisungen können generell oder im Einzelfall erteilt werden.

## Zu § 9 Absatz 2

§ 126 b BGB erlaubt eine schriftliche Erklärung ohne eigenhändige Unterschrift oder qualifizierte elektronische Signatur. Dadurch wird der Einsatz neuer Techniken (Fax, Computerfax, E-Mail) ermöglicht.

## Zu § 9 Absatz 3

Die Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung.

## Zu § 10

Der Auftragsverarbeiter muss technisch in der Lage sein, die vertraglich vereinbarte Löschung datenschutzkonform umzusetzen.

## Zu § 10 Absatz 1

Es empfiehlt sich, die Maßnahmen zur Vernichtung der Papierdokumente der Datenträger konkret festzulegen. Die erforderlichen Maßnahmen richten sich nach den jeweils aktuellen DIN-Normen sowie dem Maßnahmenkatalog des BSI. Sofern keine Beschreibung in der Anlage 1 dieser Vereinbarung erfolgt, wäre ggf. folgender Textvorschlag aufzunehmen:

*„Nach Aufforderung des Auftraggebers werden zu vernichtende Papierdokumente mit personenbezogenen Daten vom Auftragsverarbeiter ordnungsgemäß nach Maßgabe der jeweils aktuellen DIN 66399, Sicherheitsstufe 3 bis 7, entsorgt.*

*Das Löschen von Datenträgern erfolgt, sofern der Datenträger hierbei vernichtet werden muss, durch Schreddern oder Zerfasern nach Maßgabe der jeweils aktuellen DIN 66399. Dies gilt auch für bei der Datenverarbeitung durch den Auftragsverarbeiter entstandene Zwischendaten, Arbeitsdateien und sonstiges Ausschussmaterial. Der Auftraggeber ist berechtigt, die Vernichtung bzw. Löschung personenbezogener Daten beim Auftragsverarbeiter zu überwachen.“*