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

zwischen

Einrichtung / Bezeichnung:	
Ansprechpartner:	
Straße, Nr.:	
PLZ, Ort:	

- nachfolgend bezeichnet als „Auftraggeber“ –

und

Evangelisch-Lutherischen Kirche in Bayern
Landesbischof Christian Kopp
Katharina-von-Bora-Straße 7-13
80333 München

- nachfolgend bezeichnet als „Auftragsverarbeiter“ -

Begriffsbestimmungen

Hauptvertrag bezeichnet den zwischen den Parteien geschlossenen Vertrag zur Bereitstellung einer Musterwebsite von Vernetzte Kirche.

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 der auftraggebenden kirchlichen Stelle.

Auftragsverarbeitungsvertrag (kurz: **AVV)** bezeichnet den vorliegenden Vertrag zur Regelung der Auftragsverarbeitung. Paragrafen 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 die auftraggebende kirchliche Stelle an den Auftragsverarbeiter übergibt, als auch Daten, die im Auftrag der auftraggebenden kirchliche Stelle erstmalig durch den Auftragsverarbeiter erhoben werden. Dieser Vertrag gilt für alle Tätigkeiten und Anwendungen, bei denen Mitarbeitende des Auftragsverarbeiters oder – so weit die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle nach deren Weisung:

Bereitstellung einer Instanz einer Musterwebsite auf den Servern der Abteilung Vernetzte Kirche / Intranet der Evangelischen Landeskirche in Bayern, die durch die Firma Ionos bereitgestellt werden.

Bereitstellung des Webspace für die Musterwebsite (Hosting)

Aktualisierung der Grundprogrammierung (Wartung und Updates)

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

§ 2
Konkretisierung des Auftragsinhalts

(1) Die auftraggebende kirchliche Stelle 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:

Personenbezogene Daten, die in das Content-Management durch den Auftraggeber eingepflegt werden (Website-Inhalte).

Daten, die über das ggfs. vorhandene Kontaktformular an den Auftraggeber per E-Mail geschickt werden.

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

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

-

bzw. werden wie folgt näher beschrieben:

-

3. Kreis der betroffenen Personen

Der Kreis der im Rahmen dieses Auftrags durch den Umgang mit ihren personenbezogenen Daten betroffenen Personen umfasst

Gemeindeglieder, haupt-, neben- und ehrenamtliche Mitarbeitende der Einrichtung / Gemeinde, Besucher der Website

§ 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 der auftraggebenden kirchlichen Stelle sein jeweils aktuelles IT-Sicherheitskonzept zur Verfügung.

(2) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen der auftraggebenden kirchlichen Stelle 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 die auftraggebend

kirchliche Stelle unverzüglich benachrichtigen, soweit er beabsichtigt wesentliche Anpassungen vornehmen.

(3) Der Auftragsverarbeiter ist verpflichtet, der auftraggebenden kirchlichen Stelle 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. Die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchliche Stelle, garantiert der Auftragsverarbeiter, dass diese Daten durch technische und organisatorische Maßnahmen von den Daten der auftraggebenden kirchlichen Stelle getrennt sind und bleiben.

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

§ 4
Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter hat nur nach Weisung der auftraggebenden kirchlichen Stelle 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 der auftraggebenden kirchlichen Stelle 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 die auftraggebende kirchliche Stelle verweisen. Der Auftragsverarbeiter wird das Ersuchen der betroffenen Person unverzüglich an die auftraggebende kirchliche Stelle weiterleiten.

(3) Ist die auftraggebende kirchliche Stelle gegenüber einer betroffenen Person verpflichtet, dieser Auskünfte zur Auftragsverarbeitung zu erteilen, wird der Auftragsverarbeiter auf eigene Kosten die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchlichen Stelle 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 der auftraggebenden kirchlichen Stelle 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. Der auftraggebenden kirchlichen Stelle 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 die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle 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) Der auftraggebenden kirchlichen Stelle 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 der auftraggebenden kirchlichen Stelle nachzuweisen.

(7) Die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchlichen Stelle. 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 die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchliche Stelle unverzüglich schriftlich mitzuteilen.

§ 6
Unterauftragsverhältnisse

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

Keine

(2) Die Verträge des Auftragsverarbeiters mit seinen Unterauftragnehmern sind derart gestaltet, dass sie den Anforderungen der gem. § 5 Absatz 1 jeweils anwendbaren gesetzlichen Bestimmungen über den Datenschutz genügen und dass die Unterauftragnehmer unmittelbar gegenüber der auftraggebenden kirchlichen Stelle 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 der auftraggebenden kirchlichen Stelle 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 der auftraggebenden kirchliche Stelle. Holt der Auftragsverarbeiter im Falle einer weiteren Unterbeauftragung entgegen § 6 Absatz 3 Satz 1 die vorherige Zustimmung der auftraggebenden kirchlichen Stelle nicht ein, berechtigt dies die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchlichen Stelle auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 7
Kontrollrechte der auftraggebenden kirchlichen Stelle

(1) Die auftraggebende kirchliche Stelle hat das Recht, die nach § 30 Absatz 3 Satz 3 vorgesehene Überprüfung durchzuführen oder durch im Einzelfall zu benennende Personen durchführen zu lassen. Sie 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, der auftraggebenden kirchlichen Stelle 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 der auftraggebenden kirchlichen Stelle nach § 30 Absatz 3 Satz 3 DSG-EKD und im Wege der Datenschutz-Folgenabschätzung nach § 34 DSG-EKD stellt der Auftragsverarbeiter sicher, dass sich die auftraggebende kirchliche Stelle von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter der auftraggebenden kirchlichen Stelle 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 EKD zu.

§ 8
Informations- und Unterstützungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter wird die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchliche Stelle. 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. Die auftraggebende kirchliche Stelle ist über die getroffenen Maßnahmen zu informieren.

(2) Über Maßnahmen von Strafverfolgungsorganen wird der Auftragsverarbeiter die auftraggebende kirchliche Stelle unaufgefordert und unverzüglich benachrichtigen, soweit hierdurch die Datenverarbeitung für die auftraggebende kirchliche Stelle 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 EKD wird der Auftragsverarbeiter die auftraggebende kirchliche Stelle unaufgefordert unverzüglich in Kenntnis setzen, sofern hierdurch die Datenverarbeitung für die auftraggebende kirchliche Stelle betroffen ist.

§ 9
Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Die auftraggebende kirchliche Stelle behält sich im Rahmen der gemäß dem AVV durchgeführten Auftragsverarbeitung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass sie durch Einzelweisungen konkretisieren kann. Der Auftragsverarbeiter wird die Weisungen der auftraggebenden kirchlichen Stelle 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 die auftraggebende kirchliche Stelle unverzüglich schriftlich oder in Textform (§ 126b BGB) bestätigen.

(3) Der Auftragsverarbeiter hat die auftraggebende kirchliche Stelle 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 bei der auftraggebenden kirchlichen Stelle bestätigt oder geändert wird. Über seine Bedenken hat er die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle, spätestens jedoch mit der Beendigung des Hauptvertrages hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der auftraggebenden kirchliche Stelle auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Vervielfältigungen der Daten der auftraggebenden kirchlichen Stelle (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 der auftraggebenden kirchlichen Stelle 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.

	Evangelische Landeskirche in Bayern; Vernetzte Kirche / Intranet
Bezeichnung des Auftraggebers	Bezeichnung des Auftragsverarbeiters
	München, 9.7.2021
Ort, Datum	Ort, Datum
	M. Geyer Abteilungsleiter
Unterschrift mit Funktionsbezeichnung	Unterschrift mit Funktionsbezeichnung

Anlage 1:
Technische und organisatorische Maßnahmen des Auftragnehmers

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.

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSG-EKD.

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem DSG-EKD eingesetzt.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Ein Datenschutzbeauftragter zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem DSG-EKD ist bestellt. Kontaktdaten: Mareike Gotter Katharina-von-Bora-Straße 7-13 80333 München
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung durch den Datenschutzbeauftragten.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen des internen Verfahrensverzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DSG-EKD nachgewiesen. Eventuell notwendige Vorabkontrollen werden schon im Planungsstadium integriert.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DC-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Alle Mitarbeiter des Anbieters haben zu jeder Zeit Zugang zu den allgemein zugänglichen Räumlichkeiten der Organisation. Zutritte zu anderen Sicherheitszonen (z.B. Serverraum der intern

Nr.	Gebiet	Beschreibung
		genutzten DV-Anlagen) werden nur auf Anforderung und nach Freigabe durch einen Freigabeberechtigten freigeschaltet. Die Überprüfung der Zutrittsberechtigungen erfolgt in regelmäßigen Abständen. Als Besucher gelten alle Personen, die nicht Mitarbeiter des Evangelischen Presseverbands für Bayern e.V. sind. Alle Besucher werden im Haus begleitet. Alle externen Handwerker und Haustechniker müssen sich zu Beginn ihrer Arbeiten bei ihrem Ansprechpartner melden. Dieser veranlasst die Abholung am Empfang bzw. der Eingangstüre. Ist weder der gewünschte Mitarbeiter noch ein anderer Mitarbeiter, der mit der Aufgabe für den externen Handwerker oder Haustechniker vertraut ist, erreichbar, darf kein Zutritt gewährt werden.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume sind mit einer Sicherheits-Schließanlage ausgerüstet.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	In den Büroräumlichkeiten befindliche Datenverarbeitungsanlagen werden durch Kennwörter geschützt. Die Räumlichkeiten sind nach Büroschluss verschlossen.
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur sehr selektiv und nur nach Genehmigung durch die IT-Abteilung vergeben. Rechtevergabe und Änderung sind dokumentiert. Zugriff auf kaufmännische Dokumente und Kommunikationsinformationen sind durch Passwörter geschützt.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision der vergebenen Rechte ist Teil der Prüfungen der Maßnahmen und wird zusammen mit dem Datenschutzbeauftragten durchgeführt und von diesem dokumentiert.
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Die Anlage und Veränderung von Benutzerzugängen wird dokumentiert (per Anweisung durch den Abteilungsleiter oder den CIO per E-Mail).
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, vor allem an den Grundsatz der Datenvermeidung und Datensparsamkeit. Änderungen bedürfen der Anweisung durch den Vorstand.

Nr.	Gebiet	Beschreibung
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Ein Zugang zur Fernwartung der Systeme ist per verschlüsselter VPN-Verbindung nur für die Administration und den IT-Dienstleister verfügbar.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden in einem geschützten Bereich gespeichert.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben „Empfehlungen des BSI“ dienen als Vorbild für die o.g. Systemeinstellungen.
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Durch Systemeinstellungen.
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten.
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt Vergabe von Benutzerzugängen in Punkt 1.2; die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur.
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Durch regelmäßige Reports aus dem Berechtigungssystem.
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Durch eine stichprobenartige Durchsicht der Systemprotokolle durch die IT-Abteilung.
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter. Ausschließlich die Geschäftsführung und der IT-Mitarbeiter; das 4-Augen-Prinzip findet im Falle der Auswertung Anwendung.
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Die Überprüfung, ob eine Trennung von Daten und Funktionen notwendig ist, wird bei der Auswahl und Implementierung von Systemen berücksichtigt und wenn gegeben eingehalten, dokumentiert und überprüft.
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden bzw. werden

Nr.	Gebiet	Beschreibung
	Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung.
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	Bei der Erhebung und Verarbeitung von personenbezogenen Daten wird geprüft, ob der Personenbezug notwendig ist oder notwendige Informationen auch pseudonymisiert zur Weiterverarbeitung / Speicherung ausreichen. Dies wird vor allem auch im Bereich der Logdaten berücksichtigt. Ist in besonderen Fällen aber der Rückschluss auf Personenbezug notwendig, wird der Personenbezug durch geeignete Maßnahmen wiederhergestellt.
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Eine Weitergabe der Daten zur Weiterverarbeitung an Dritte erfolgt nur in Absprache mit dem Kunden oder gemäß Weisung des Kunden. Defekte Datenträger werden durch Fachunternehmen verschrottet, dieser Vorgang wird dokumentiert.
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Unternehmensintern werden Daten auf mobilen Datenträgern je nach Informationsklassifizierung / Einsatzart verschlüsselt gespeichert. Eine Verschlüsselung von Datenträgern des Kunden erfolgt nach Vorgabe des Kunden.
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine Firewall und eine strikte Rechtevergabe sichern die Daten vor unberechtigtem Zugriff aus dem Internet bzw. aus dem Hausnetz.
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Dies wird im Rahmen der Kontrollen unter Punkt 1 mit geprüft.
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Durch den Einsatz von Systemen mit Protokollfunktionen. Die Aufbewahrung von Systemprotokollen erfolgt gemäß den gesetzlichen Vorgaben.
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Durch Rollen-/Rechtekonzepte und diverse Lizenzmodelle mit unterschiedlichen Berechtigungskonzepten.
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechtekonzepts zur ordnungsgemäßen Datenverarbeitung und Speicherung.

Nr.	Gebiet	Beschreibung
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge werden bei Bedarf geschlossen. Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftrage des Unternehmens. Er ist auch bei der Auswahl der beauftragten Firmen maßgeblich beteiligt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten (Sicherungsbänder) sind räumlich getrennt von Produktivdaten in einem Brandschutzabschnitt gelagert.
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Durch physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung.
3.2.	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Eingerichtetes 2-stufiges Backup-Verfahren. Wiederherstellung der Datenstände der vergangenen 14 Tage auf Zuruf; Sicherung älterer Datenstände durch Einspielen von Bändern.
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident - Response-Management)?	Die Sicherheitsvorfallbehandlung ist eng mit den betrieblichen Prozessen verzahnt. Sowohl Messverfahren als auch Alarmierung, Meldung, Reaktion, Eskalation und Dokumentation sind unter Berücksichtigung der Vorgaben implementiert.

Nr.	Gebiet	Beschreibung
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen.
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsverarbeitung gestaltet. Der Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr.

Anlage 2:
Berechtigte Weisungsgeber und Weisungsempfänger, Datenschutzbeauftragte

(1)
Zur Erteilung von Weisungen betreffend die Auftragsverarbeitung sind auf Seiten der auftraggebenden kirchlichen Stelle folgende Personen berechtigt:

(*Name, Funktion, Anschrift, Telefon, Fax, E-Mail)*

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

(2)
Zum Empfang von Weisungen betreffend die Auftragsverarbeitung sind aufseiten des Auftragsverarbeiters ausschließlich folgende Personen berechtigt:

Miklós Geyer

Referent Vernetzte Kirche / Intranet

Evangelisch-Lutherische Kirche in Bayern

Abteilung I6

Katharina-von-Bora-Str. 7-13

80333 München

(3)
Beim Auftragsverarbeiter ist

Mareike Gotter, Katharina-von-Bora-Straße 7-13, 80333 München

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

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

(4)
Bei der auftraggebenden kirchlichen Stelle ist folgende Person

[Name und Kontaktdaten]

als örtlich Beauftragte(r) für den Datenschutz bestellt.

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 die auftraggebende kirchliche Stelle 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 der auftraggebenden kirchlichen Stelle und nicht als Dritter behandelt wird, verbleibt auch die Verantwortlichkeit bei der auftraggebenden kirchlichen Stelle. Sie ist insbesondere 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 die auftraggebende kirchliche Stelle 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 insbesondere 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 der auftraggebenden kirchlichen Stelle dar.

Die auftraggebende kirchliche Stelle 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 (inklusive 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 der auftraggebenden kirchlichen Stelle 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 Paragrafen 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 der auftraggebenden kirchlichen Stelle; zum einen bei effektiven Maßnahmen der Wahrnehmung ihrer Kontrollrechte gegenüber dem Auftragsverarbeiter; zum anderen kann sie von der auftraggebenden kirchlichen Stelle herangezogen werden, um ihrer Nachweispflicht aus § 5 Absatz 2 DSG-EKD nachzukommen.

Zu § 3 Absatz 1 Satz 5

Bei der Verarbeitung personenbezogener Daten ist von der auftraggebenden kirchlichen Stelle der Schutzbedarf festzulegen. Bei einem hohen oder sehr hohen Schutzbedarf der personenbezogenen Daten ist ein IT-Sicherheitskonzept vorzulegen. In anderen Fällen, insbesondere wenn der Schutzbedarf der personenbezogenen Daten als normal 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 und 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.

Zu § 4 Absatz 2

Bei der Auftragsverarbeitung bleibt die auftraggebende kirchliche Stelle 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-Datenschutzgrundverordnung 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 von der auftraggebenden kirchlichen Stelle regelmäßig durchzuführenden Datenschutzkontrollen einzubeziehen sind. Mit Blick auf Kontrollen

am Dienstsitz des Auftragsverarbeiters können der auftraggebenden kirchlichen Stelle daher im Vergleich zur Auftragsverarbeitung innerhalb Deutschlands erhebliche organisatorische und wirtschaftliche Mehraufwände entstehen.

Die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle, 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 der auftraggebenden kirchlichen Stelle 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 die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle 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 die auftraggebende kirchliche Stelle 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

Die auftraggebende kirchliche Stelle 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 die auftraggebende Stelle und den Auftragsverarbeiter die Meldepflicht aus §§ 32 DSG-EKD. Die dem Auftragsverarbeiter gem. § 8 aufzuerlegenden Pflichten dürfen keinesfalls hinter den in § 32 Abs. 2 DSG-EKD gesetzlichen Pflichten des Auftragsverarbeiters zurückbleiben. Die auftraggebende kirchliche Stelle 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-DSGVO bzw. BDSG) 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 der auftraggebenden kirchlichen Stelle 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. Die auftraggebende kirchliche Stelle ist berechtigt, die Vernichtung bzw. Löschung personenbezogener Daten beim Auftragsverarbeiter zu überwachen.“