Vertrag zur Auftragsverarbeitung von personenbezogenen Daten

zwischen

_____

Institution (Kirchengemeinde, Kirchenbezirk, Kirchenkreis, Einrichtung, Verein oder Projektstelle)

_____

Ggf. Träger/Kirchenbezirk, Kirchenkreis, zu dem Ihre Institution gehört

_____

Kundennummer (falls bekannt)

_____

Straße und Hausnummer

_____

PLZ, Ort

_____

Ansprechpartner Vorname, Nachname

-nachfolgend Auftraggeber genannt-

und

Evangelisches Medienhaus GmbH
Augustenstraße 124
70197 Stuttgart

-nachfolgend Auftragsverarbeiter genannt-

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

zwischen

Auftraggeber lt. Deckblatt

und

Evangelisches Medienhaus GmbH

Augustenstrasse 124

70197 Stuttgart

(nachfolgend bezeichnet als „Auftragsverarbeiter“)

Begriffsbestimmungen

„Hauptvertrag“ bezeichnet den zwischen den Parteien geschlossenen Vertrag (Bestellung Baukasten).

„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.

„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 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 – soweit 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:

a. Bereitstellung von Vorlagen (Baukasten) zur Erstellung einer Website auf Basis eines Redaktionssystems

b. Hosting der Website sowie Wartung und Weiterentwicklung des Redaktionssystems

c. Unterstützung und Beratung bei der Erstellung der Website und der Arbeit im Redaktionssystem

d. Auf gesonderten Antrag: Bereitstellung eines Systems zur Pflege und Veröffentlichung von Veranstaltungen und Ressourcen (amosWEB), Unterstützung in der Anwendung

e. Auf gesonderten Antrag: Unterstützung bei Erstellung und Versand von Newslettern

(2) Diese Vereinbarung gilt ab dem Vertragsabschluss des Hauptvertrags und endet nach der Beendigung des Hauptvertrages mit der Übergabe oder der Vernichtung aller personenbezogenen Daten der auftraggebenden kirchliche 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:

Es werden einfache personenbezogene Daten verarbeitet, nämlich

- Name, Vorname, Adresse
- Kontaktdaten
- Bilddaten, Videodaten, Audiodaten
- Zugriffsdaten Internet
- E-Mailadressen der Newsletterempfänger

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:

Siehe §1 Absatz 1 dieses Vertrages

Die Unterstützungsleistung erfolgt per E-Mail oder telefonisch, in Einzelfällen auch persönlich oder per Fernwartungssoftware. Um die Anfragen bearbeiten zu können, erfolgt bei Bedarf ein Zugriff auf die Benutzerumgebung des Auftraggebers über den Admin-Zugang des Auftragnehmers. Jegliche Unterstützungsleistung erfolgt ausschließlich nach Anforderung durch den Auftraggeber.

- Daten des Auftraggebers werden vom Auftragnehmer nur zur Vertragserfüllung verarbeitet und nicht an Dritte weitergegeben.
- Die Internetseiten des Auftraggebers werden auf dem Server des Dienstleisters des Auftragnehmers gespeichert.
- Bei Bedarf unterstützt der Auftragnehmer bei der Erstellung des Internetauftritts, des Newsletters und im Umgang mit den Softwareanwendungen, wodurch auch die dort vom Auftraggeber eingegebenen Personendaten ersichtlich sind.
- Der Auftragnehmer wird Daten nur dann ändern oder löschen, wenn er vom Auftraggeber dazu angewiesen ist.

3. Kreis der betroffenen Personen

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

- Besteller (Auftraggeber des Baukastens)
- Webmaster (Haupt- und Ehrenamtliche)
- Verantwortliche im Impressum
- Ansprechpartner bzw. Handelnde des Auftraggebers

§ 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 wurden, trägt der Auftragsverarbeiter die mit den technischen und organisatorischen Maßnahmen verbundenen Kosten.

(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 auftraggebende 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 kirchliche Stelle getrennt sind und bleiben.

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

§ 4
Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter hat nur nach Weisung der auftraggebenden kirchliche 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 kirchliche 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 kirchliche Stelle wird der Auftragsverarbeiter die Verpflichtung der Beschäftigten und sonstigen Personennachweisen.

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 kirchliche 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 kirchliche Stelle sind die Prüfprotokolle auf Verlangen unverzüglich vorzulegen.

(4) 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.

(5) 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 kirchliche Stelle nachzuweisen.

(6) 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.

(7) Die Verarbeitung im Auftrag außerhalb der Betriebsstätte des Auftragsverarbeiters (z. B. Home-Office und mobiles Arbeiten) ist gestattet, vorausgesetzt der Auftragsverarbeiter gewährleistet die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch aus dieser Arbeitsorganisation heraus. Der Auftragsverarbeiter trägt insbesondere Sorge dafür, dass eine integre Verarbeitung personenbezogener Daten sowie eine wirksame Kontrolle der Verarbeitung im Auftrag außerhalb der Betriebsstätte sichergestellt ist. Die Parteien sind sich darüber einig, dass regelmäßige Kontrollmaßnahmen außerhalb der Betriebsstätte dem Auftragsverarbeiter obliegen, um die Persönlichkeitsrechte der Beschäftigten des Auftragsverarbeiters oder etwaigen Dritten zu wahren. Anlassbezogen ist der auftraggebenden kirchlichen Stelle eine Vor-Ort-Kontrolle zu ermöglichen. Birgt die Verarbeitung im Auftrag ein bestimmtes hohes Risiko für die Rechte natürlicher Personen (beispielsweise Risikoanalyse, Datenschutz-Folgenabschätzung), ist die Datenverarbeitung nur in den Betriebsstätten des Auftragsverarbeiters durchzuführen.

(8) 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:

Unterauftragnehmer	**Verarbeitungsstandort**	**Art der Leistung**
B-Factor GmbH, Stuttgart Sigmaringer Str. 98 70567 Stuttgart 0711-18420280	Deutschland	Entwicklung und Wartung Baukasten-Redaktionssystem
Connecta AG, Wiesbaden Rheinstraße 1 65189 Wiesbaden 0611-34109-0	Deutschland	Hosting Baukastensystem und Statistiksoftware
Bei Nutzung der Newsletterfunktion: CleverReach GmbH & Co. KG Schafjückenweg 2 26180 Rastede	Deutschland Irland	Newsletterverwaltung
Bei Nutzung von amosWEB: Evangelisches Jugendwerk in Württemberg Haeberlinstraße 1-3 70563 Stuttgart	Deutschland	Entwicklung, Wartung und Hosting amosWEB

(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 kirchliche 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 kirchliche Stelle in Kopie zu übergeben. Die mit den Unterauftragnehmern ausgehandelten Preise können geschwärzt werden.

(3) Über 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 wird der Auftraggeber informiert.

Die auftraggebende kirchliche Stelle ist in diesem Fall zur außerordentlichen Kündigung des Vertrags mit dem Auftragsverarbeiter berechtigt.

(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 kirchliche 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 kirchliche 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 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, das sie durch Einzelweisungen konkretisieren kann. Der Auftragsverarbeiter wird die Weisungen der auftraggebenden kirchliche 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 kirchliche 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 kirchliche 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.

Evangelisches Medienhaus GmbH

Evangelisches Medienhaus GmbH
Augustenstraße 124
70197 Stuttgart
Tel. 0711 22276-0
Fax 0711 22276-43
evmedienhaus.de

(Ort, Datum)

Stuttgart, 20. Dezember 2023

(Unterschrift Auftraggeber)

Frank Zeithammer, Geschäftsführer

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.

Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen	
1. Pseudonymisierung	• Zur internen Zuordnung werden Kundennummern verwendet
2. Verschlüsselung	• Verschlüsselungsmethoden werden stets auf dem aktuellem Stand der Technik gehalten • Alle Datenträger von firmeninternen Notebooks oder PCs sind grundsätzlich per XTS-AES 128-bit (BitLocker) verschlüsselt. Für andere OS-Systeme wird ein entsprechend ähnliche Methode verwendet • Mobilgeräte kommunizieren mit dem internen Netzwerk ausschließlich über eine verschlüsselte Verbindung • E-Mails mit sensiblem Inhalt werden verschlüsselt • Mobile Datenträger werden auf dem Transportweg verschlüsselt • Backup Datenträger sind grundsätzlich mit einem Passwort versehen • Öffentlich zugängliche Webseiten verfügen stets über eine aktuelle Verschlüsselung per SSL (https:) • Für Adminzugänge sind sog. Mehrstufige Authentifizierungen vorgesehen
3. Vertraulichkeit	• Es besteht ein interner On- und Offboarding Prozess für die Vergabe, Änderung und den Entzug von IT-Berechtigungen. Berechtigungen werden mind. einmal jährlich überprüft und ggf. angepasst • Für alle relevanten Anwendungen bestehen Berechtigungskonzepte, die nach dem Need-to-Know-Prinzip erstellt wurden • Es existieren abgestufte Schließkreise mit unterschiedlichen Zutrittsberechtigungen • Zutritt zu neuralgischen Räumen erhält nur ein kleiner Personenkreis, dies wird auch elektronisch mit Sensoren überwacht • Es besteht ein Prozess zur Vergabe, Veränderung und zum Entzug von Schließberechtigungen • Der Serverraum wird hinsichtlich diverser Faktoren überwacht: Temperatur, Feuchtigkeit, Bewegung und Rauch. Zusätzlich ist dieser Alarmgesichert • Zugriffsmöglichkeiten auf Daten werden auf das erforderliche Maß beschränkt, Grundlage hierfür ist das allgemeine Berechtigungskonzept

	• Es bestehen Vorgaben für Länge und Komplexität von Kennwörtern, die nach Möglichkeit technisch erzwungen werden. die jederzeit technisch erzwungen werden. Zusätzlich wird der User in regelmäßigen Abständen gezwungen sein Passwort zu verändern, hierbei können die letzten fünf Passwörter nicht recycelt werden • Auf Client-Systemen wird eine Bildschirmsperre erzwungen • Multifaktorauthentifizierung wird für alle UserInnen und Admins erzwungen • Adminzugänge sind in diverse Schichten unterteilt und existieren für separate Server. Für neuralgische Systeme sind extra abgesicherte Zugänge vorhanden, die teilweise durch physische Trennung gehärtet sind. • Das Backup wird nach dem Prinzip 3-2-1-0 durchgeführt • Ein aktives Monitoring/Alterting ist eingerichtet und verschickt proaktiv Meldungen über definierte Zustände der Sensoren mit Warnungen/Fehlern
4. Verfügbarkeit	• Für Systeme mit hohen Verfügbarkeitsanforderungen existieren Ausweichsysteme und automatisierte Prozessstandards. Bei neuralgischen Systemen besteht jederzeit eine Redundanz • Endpointsysteme werden jederzeit auf dem aktuellen Stand gehalten und werden ASAP nach Bekanntwerden von Sicherheitslücken mit dem vom Hersteller bereitgestellten Update oder Workaround versehen. • Firewallsysteme werden jederzeit auf dem aktuellen Stand gehalten und werden ASAP nach Bekanntwerden von Sicherheitslücken mit dem vom Hersteller bereitgestellten Update oder Workaround versehen. • Die Ersatzbeschaffung von Hardware ist regelmäßigen Zyklen unterworfen und ist nach Kritikalität des Systems eingestuft • Entsprechende Maintance-Verträge mit Herstellern oder Partnern existieren • Daten werden mehrfach täglich gesichert. Ein ausführliches Backupkonzept mit der Regel 3-2-1-0 existiert und wird regelmäßig mit Wiederherstellung-Stichproben validiert. Stichwort: Rücksicherung und Reliabilität. • Für neuralgische IT-Systeme existieren Service-Level-Agreements mit externen Partnern. • Es werden nur standardisierte IT-Systeme eingesetzt (Hard- und Software)
5. Belastbarkeit	• Für alle IT-Systeme werden ausreichend Ressourcen mit Hinblick auf CPU, RAM und Storage Ressourcen zur Verfügung gestellt. Diese Ressourcen werden aktiv überwacht und bei Warn- oder Fehlerschwellen entsprechend händisch oder teilautomatisiert angepasst. • Server- und Clientsysteme werden regelmäßig hinsichtlich ihrer Belastbarkeit überprüft. Stichwort: Stresstest und Sicherheitsaudits. • Ein System für Incident-Response-System und -Plan ist eingerichtet
6. Physischer oder technischer Zwischenfall	• Sicherung von Serverraum durch physische- und elektronische Zugangskontrollen

	• Einsatz von Umweltkontrollsystemen. Redundante Klimasteuerung, Temperaturkontrollen, Brandschutz im kompletten Serverraum • Bei stromtechnischen Zwischenfällen ist das Rechenzentrum mit entsprechenden Batterien (USVs) versehen. Im Worst-Case wird das Rechenzentrum komplett automatisiert heruntergefahren, um Schäden an Hardware und Verlust von Daten vorzubeugen • Ein robuster Notfallplan inkl. Ersatzressourcen ist vorhanden. Stichwort: Notfallhandbuch, Shutdown und Wiederanlaufpla • Ein Prozess für den Umgang mit Sicherheitsvorfällen ist definiert • Es besteht ein Konzept zum Umgang mit Datenpannen
7. Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM	• Der Schutzbedarf von IT-System und Daten wird mind. einmal jährlich überprüft. Bei neuralgischen Systemen findet dieser Prozess dauerhaft statt • Das Schutzniveau von Anwendungen wird mind. einmal jährlich überprüft. Bei neuralgischen Systemen wird dieses Niveau dauerhaft überprüft und ist teilweise an Partner ausgelagert, die dafür spezialisiert sind. Beispiel: Sicherheitslücken in Firewall Hard- oder Software • In regelmäßigen Abständen finden interne Auditierungen statt, die der DIN ISO 27001 entsprechen • Datenschutzvorfälle werden stets dokumentiert und hinsichtlich ihrer Daten, des Risikos und der Auswirkung auf die jeweilige Personengruppe hin ausgewertet. • Es finden regelmäßige Reviews und Arbeiten zur Optimierung von IT-Systemen statt. Bei neuralgischen Systemen wird in der Regel auf einen spezialisierten Partner zurückgegriffen
8. Löschverfahren nach § 10 Abs. 1	• Nach Beendigung des Auftragsverarbeitungsverhältnisses werden die Daten manuell gelöscht. Eine gesetzliche Aufbewahrungsfrist bleibt unberührt.

Anlage 2: Berechtigte Weisungsgeber und Weisungsempfänger, Datenschutzbeauftragte

Die Ansprechpartner mit Weisungsbefugnis und die Weisungsempfänger werden zwischen Auftraggeber und Auftragnehmer abgestimmt.

Beim Auftragsverarbeiter ist Roland Hübner als örtlich Beauftragter für den Datenschutz bestellt.

Bei der auftraggebenden kirchlichen Stelle ist folgende Person

_____

Name und Kontaktdaten

als örtlich Beauftragte(r) für den Datenschutz bestellt.