Vertrag zur Auftragsverarbeitung von personenbezogenen Daten

zwischen

_____

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

_____

Ggf. Träger/Kirchenbezirk, 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 Auftragnehmer genannt-

1. Gegenstand und Dauer der Vereinbarung

Der Vertrag regelt die Rechte und Pflichten der Vertragsparteien aufgrund der anzuwendenden Datenschutzgesetzte.

Der Auftrag umfasst Folgendes (Zweck der Verarbeitung):

- Bereitstellung von Vorlagen (Baukasten) zur Erstellung einer Website auf Basis eines Redaktionssystems
- Hosting der Website sowie Wartung und Weiterentwicklung des Redaktionssystems
- Unterstützung und Beratung bei der Erstellung der Website und der Arbeit im Redaktionssystem
- Bereitstellung eines Systems zur Pflege und Veröffentlichung von Veranstaltungen und Ressourcen (Onlineplaner), Unterstützung in der Anwendung sowie Hosting der Daten
- Auf gesonderten Antrag: Unterstützung bei Erstellung und Versand von Newslettern

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. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne der anzuwendenden Datenschutzgesetze. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union erbracht.

Der Vertrag wird auf unbestimmte Zeit geschlossen. Das Vertragsverhältnis kann ohne Angabe von Gründen von beiden Seiten mit einer Frist von zwei Monaten zum 30. Juni oder 31. Dezember gekündigt werden.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Der Zweck der Verarbeitung ist in Absatz 1 aufgeführt.

Art der Verarbeitung:

- 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.

Art der personenbezogenen Daten:

Es werden einfache personenbezogene Daten verarbeitet, nämlich

- Name, Vorname, Adresse
- Kontaktdaten
- Bilddaten, Videodaten
- Zugriffsdaten Internet
- E-Mailadressen der Newsletter-Empfänger

Kategorien betroffener Personen:

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

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Für die Einhaltung der Datenschutzpflichten zwischen Auftraggeber und dessen haupt- und ehrenamtlichen Mitarbeiterinnen und Mitarbeitern ist alleine der Auftraggeber verantwortlich und trifft die dafür erforderlichen Maßnahmen.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und zu dokumentieren.

Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend vom Auftraggeber zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftraggeber dies verlangt.

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Der Auftraggeber ist für die Richtigkeit der Angaben in Impressum und Datenschutzerklärung sowie für die Einhaltung der Datenschutzbestimmungen bezüglich der Informationspflicht und der Erfüllung von Rechten der betroffenen Personen selbst verantwortlich.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

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

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Bei der Erfüllung der Rechte der betroffenen Personen durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutzfolgenabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen. Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die vom Auftraggeber zu nennende Stelle weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren.

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mit- wirkt.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutz- rechtlichen Vorschriften bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz Herr Roland Hübner benannt.

Herr Hübner ist per E-Mail an datenschutzbeauftragter@evmedienhaus.de erreichbar. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten angemessen

zu unterstützen. Meldungen an Aufsichtsbehörden oder Betroffene für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet. Diese Genehmigung wird mit der Vertragsunterschrift erteilt und gilt auch für künftige Änderungen.

Der Auftragsnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Bei einem Einspruch kann der Auftragnehmer den Vertrag kündigen.

Der Auftragnehmer muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählt.

Eine Beauftragung von Subunternehmern in Drittstaaten findet nicht statt.

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Die Kosten für beauftragte Prüfer trägt der Auftraggeber.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Daten- schutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer folgende Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt:

Unterauftragnehmer	**Verarbeitungsstandort**	**Art der Dienstleistung**
B-Factor GmbH, Stuttgart	Deutschland	Entwicklung und Wartung Baukasten-Redaktionssystem
Connecta AG, Wiesbaden	Deutschland	Hosting Baukastensystem und Statistiksoftware
Amedick & Sommer GmbH, Stuttgart	Deutschland	Entwicklung, Wartung und Hosting Onlineplaner

Nur für Kunden mit Newsletterfunktion:		
CleverReach GmbH & Co. KG, Rastede	Deutschland Irland	Newsletterverwaltung

Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

8. Technische und organisatorische Maßnahmen

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Eine Liste der technisch organisatorischen Maßnahmen die der Auftragnehmer umgesetzt hat ist aus der Anlage ersichtlich.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten.

10. Sonstiges

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum	Ort, Datum
_____	Stuttgart, 2. Mai 2018
Unterschrift Auftraggeber	Auftragnehmer
_____	Evangelisches Medienhaus GmbH Augustenstraße 124 70197 Stuttgart Tel. 0711 22276-0 Fax 0711 22276-43 evmedienhaus.de JürgenKaiser, Geschäftsführer Wolfgang Fritz, Geschäftsführer

Anhang: Technisch-organisatorische Sicherheitsmaßnahmen

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 • Festplatten von Notebooks sind verschlüsselt, wenn Personendaten gespeichert sind • 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 • Öffentlich zugängliche Webseiten verfügen stets über eine ausreichend starke https-Verschlüsselung
3. Vertraulichkeit	• Es besteht ein Prozess für die Vergabe, Änderung und den Entzug von IT-Berechtigungen • Für alle relevanten Anwendungen bestehen Berechtigungskonzepte, die nach dem Need-to-Know-Prinzip erstellt wurden • Ein Rollenkonzept für die Berechtigungen ist realisiert • Berechtigungen werden regelmäßig auf deren Erforderlichkeit hin überprüft • Es existieren abgestufte Schließkreise mit unterschiedlichen Zutrittsberechtigungen • Es besteht ein Prozess zur Vergabe, Veränderung und zum Entzug von Schließberechtigungen • Der Serverraum wird auf Temperatur überwacht • Zugriffsmöglichkeiten auf Daten werden auf das erforderliche Maß beschränkt • Es bestehen Vorgaben für Länge und Komplexität von Kennwörtern, die nach Möglichkeit technisch erzwungen werden

4. Verfügbarkeit	• Für Systeme mit hohen Verfügbarkeitsanforderungen existieren Ausweichsysteme • Virenschutz und Firewallsysteme werden stets aktuell gehalten • Ein Plan zur Ersatzbeschaffung von Hardware ist vorhanden • Daten werden täglich inkrementell gesichert • Es werden regelmäßig Funktionstests für Rücksicherungen durchgeführt • Es werden nur standardisierte IT-Systeme eingesetzt (Hard- und Software) • Für wichtige IT-Systeme existieren Service-Level-Agreements
5. Belastbarkeit	• Für wichtige IT-Systeme werden ausreichend Ressourcen zur Verfügung gestellt
6. Physischer oder technischer Zwischenfall	• Es besteht ein Datensicherungs-Konzept • 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 der Daten wird jährlich überprüft • Das Schutzniveau der Anwendungen und Systeme wird jährlich überprüft • Es finden in regelmäßigen Abständen interne Auditierungen statt • Datenschutzvorfälle werden stets dokumentiert und ausgewertet