Vereinbarung
über die Verarbeitung personenbezogener Daten im Auftrag
(Auftragsverarbeitung gemäß Art. 28 DSGVO)

(Zusätzliche Regelungen für kirchliche Stellen in Anlage 3)

zwischen

HSP-Selbsthilfegruppe Deutschland e.V.

Sophienstr. 96b

76135 Karlsruhe

– Auftraggeber –

und

HelpMundo GmbH

Maternusstr. 44

50996 Köln

– Auftragnehmer –

Nachfolgend gemeinsam „ die Vertragsparteien “

1 Geltungsbereich

(1) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

(2) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2 Gegenstand und Dauer der Verarbeitung

(1) Der Auftrag umfasst die Bereitstellung von verschiedenen onlinebasierten Spendentechnologien des Auftragnehmers, die Speicherung der eingegebenen Spenderdaten sowie die Einbindung der Zahlungsmodule von externen Zahlungsdienstleistern.

(2) Der Vertrag wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt 3 Monate.

(3) 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.

3 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Betroffene Personen

3.1 Zweckbeschreibung

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden und zwar zu folgenden Zwecken:

- Integration eines externen Spendenformulars zur Integration in die Website des Auftraggebers oder Facebook
- Nutzung von Onepagern oder Spenden-Widgets,
- Integration in das Spendenportal HelpDirect.org
- Erstellung eines eigenen HelpShops für den Auftraggeber
- Tools zur Generierung von Spenden über das Internet

Einzelne Aufgaben und Zwecke können je nach Nutzungswunsch unterscheiden, sind aber insbesondere:

- Abwicklung der durchgeführten Spende
- Beantwortung von Fragen zum Spendenformular oder Abwicklung
- Technische Administration
- Zahlungsabwicklung
- Einbindung von Zahlungsdienstleistern wie PayPal, SOFORT oder Wirecard

3.2 Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO) und betroffene Personen

Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung

Art der Daten		Betroffene Personen
Personenstammdaten	Vorname, Nachname, Titel vollständige Anschrift	Nutzer der Spenden-technologie des Auftragnehmers
Kommunikationsdaten	E-Mail-Adresse	
Vertragsbewegungsdaten	Projektauswahl soweit vorhanden, Zahlungsdaten, je nach Zahlungsart (z.B. bei SEPA: IBAN/BIC)	

4 Der Auftragnehmer

4.1 Pflichten des Auftragnehmers

4.1.1 Allgemeine Pflichten

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor.

(2) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind und überwacht die Einhaltung dieser in seinem Betrieb. Er verpflichtet sich, auch weitere für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten (z.B. Bankgeheimnis, Fernmeldegeheimnis, Sozial- geheimnis, Berufsgeheimnis).

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Die Vertraulichkeitspflicht besteht auch nach Beendigung des Auftrages fort.

(4) 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 gemacht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit zu verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Schulungs- und Sensibilisierungsmaßnahmen sind regelmäßig – spätestens alle 12 Monate – zu wiederholen.

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

4.1.2 Unterstützungspflichten

(1) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses von Verarbeitungstätigkeiten sowie bei Durchführung von Datenschutzfolgeabschätzungen im notwendigen Umfang angemessen zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(3) 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.

4.1.3 Mitteilungspflichten

(1) 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 nach Art. 33 und Art. 34 DSGVO.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen. Auskünfte an Dritte erteilt der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber.

4.1.4 Verpflichtungen nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

(1) 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 zu löschen.

(2) Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4.1.5 Bestellung des Datenschutzbeauftragten

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

4.2 Beauftragung von Subunternehmen

(1) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.

(2) Der Auftragnehmer muss dafür Sorge tragen, dass er die Subunternehmer unter besonderer Berücksichtigung der Eignung und der von diesen getroffenen, technischen und organisatorischen Maßnahmen, im Sinne von Art. 32 DSGVO, sorgfältig auswählt. Die relevanten Prüfunterlagen sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(3) Der Auftraggeber kann der Änderung aus wichtigem Grund, innerhalb einer Frist von 2 Wochen, widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund für den Widerspruch vor und ist eine einvernehmliche Lösungsfindung zwischen den Vertragsparteien nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(4) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(5) Der Auftragnehmer hat die Einhaltung der Pflichten der Subunternehmer wie folgt zu überprüfen:

- Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) mittels eines Fragenkataloges oder einer Begehung vor Ort.
- Regelmäßige Prüfung des beim Subunternehmer eingerichteten Datenschutzkonzeptes (mindestens alle 2 Jahre)
- Regelmäßige Einholung von vorhandenen Zertifikaten über eine gültige Zertifizierung nach der DSGVO.

(6) Zurzeit sind für den Auftragnehmer, die in der Anlage 1 dokumentierten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit der Beauftragung der in Anlage 1 genannten Subunternehmer erklärt sich der Auftraggeber einverstanden.

5 Der Auftraggeber

5.1 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist nach Terminvereinbarung berechtigt, die Einhaltung der Datenschutzvorschriften sowie der vertraglichen Vereinbarungen selbst oder durch vom Auftraggeber beauftragte Dritte, gemäß Art. 28 Abs. 3 Satz 2 lit. h DSGVO, zu kontrollieren.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(4) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(5) 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.

5.2 Weisungen

(1) Die Weisungen werden zum einen durch den Vertrag festgelegt, können aber vom Auftraggeber in schriftlicher Form oder in einem elektronischen Format (Textform) geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

6 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragnehmer wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleisten. Dazu wird er insbesondere die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit sowie die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung, auf Dauer sicherstellen.

(2) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.

(3) Die abgestimmten technischen und organisatorischen Maßnahmen werden in Anlage 2 zu diesem Vertrag als verbindlich festgelegt. Hierin ist auch das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung beschrieben.

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

(5) Wesentliche Änderungen müssen die Vertragsparteien in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

7 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(2) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

8 Sonstiges

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Es gilt deutsches Recht. Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart.

(3) 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.

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

Auftragnehmer

Köln, 28.10.2020

Harald Meurer, CEO

Auftraggeber

Karlsruhe, 28.10.2020

Monica Eisenbraun

Für das elektronische Format nach Art. 28 Abs. 9 DSVGO wird keine eigenhändige Unterschrift benötigt. Der hier vom Partner hinterlegte Name genügt deshalb als Unterschrift.

Anlage 1
Auflistung von Subunternehmen

Unternehmen, Anschrift & Kontaktdaten	Beschreibung der Teilleistungen
HelpDirect e.V. **Ahrweg 107, 53347 Alfter**	Verwaltung und Support der Spenderdaten und Backend-Technologie
AGIDOS GmbH **Maternusstr. 44, 50996 Köln**	Programmierung der Datenbank und der gesamten Spendentechnologie
Creative Shopping GmbH **Maternusstr. 44, 50996 Köln**	Übernahme einzelner Programmieraufgaben innerhalb der Projekte
SSA Group LP **45BWest Wilmot Street** **201 Richmond Hill** **Ontario L4B 2P3**	Übernahme einzelner Programmieraufgaben innerhalb der Projekte
PlusServer GmbH **Hohenzollernring 72,** **50672 Köln**	Hosting der Server, Standort Köln

Anlage 2
Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen
(gemäß Artikel 32 Absatz 1 DSGVO)

Angaben zum Verantwortlichen/Auftragsverarbeiter

Firma	HelpMundo GmbH
Straße	Maternusstr. 44
PLZ/Ort	50996 Köln
Telefon	0221 – 643096-0
E-Mail-Adresse	h.meurer@helpmundo.de
Internet-Adresse	www.helpmundo.de
Gesetzliche/r Vertreter	Harald Meurer
Datenschutzbeauftragter	Es ist kein Datenschutzbeauftragter notwendig

1. Pseudonymisierung	- Die Nutzung der angebotenen Spendentechnologien und die im Zusammenhang damit erhobenen Daten sind im Kern immer personenbezogen. Die Abwicklung erfolgt für eine bestimmte Person, weshalb hier eine Pseudonymisierung nicht oder nur vereinzelt möglich ist. - Bei der Nutzung der Unternehmenseigenen Website wird der Zugriff und jeder Abruf der hinterlegten Daten protokolliert, insbesondere der Browsertyp, das Datum und die Uhrzeit des Abrufs, die Datenmenge, der Webbrowser, die anfragende Domain, die URL der verweisenden Website sowie die IP-Adresse des anfragenden Rechners. Dies erfolgt ohne konkreten Personenbezug. - Bei neuen Datenverarbeitungen wird vorab überprüft, wo eine pseudonymisierte Verwendung ausreicht und entsprechend umgesetzt werden kann.
2. Verschlüsselung	- Die Kennwörter von Bearbeitern werden als Hash mit einem Salt gespeichert. - Die Kommunikation zwischen Klient und Server findet ausschließlich verschlüsselt über HTTPS statt (TLS Verschlüsselung). - Zugriffe auf die Datenbank und Server erfolgen nur über einen sicheren SSH Zugang (TLS Verschlüsselung). - Direkte Verbindungen zum Servernetzwerk durch Mitarbeiter sind nur mittels VPN möglich.

3. Vertraulichkeit	- Zugang zum Server: Die Server befinden sich in einem Rechenzentrum der Firma PlusServer GmbH. PlusServer beschränkt den Zugang zu Einrichtungen, in denen sich ihre Informationssysteme befinden, auf eindeutig benannte autorisierte Personen. PlusServer verfügt über Verfahren, die den Zugriff auf Kopien von Kundendaten regeln (inkl. Berechtigungsmanagement). - Zugang zu Arbeitsplätzen/Endgeräten: Unsere Büros am Standort Köln sind durch eine Alarmanlage mit Polizeianbindung gesichert. Nur fest angestellte Mitarbeiter verfügen über einen Schlüssel. Mitarbeiter unserer Subunternehmer arbeiten u.a. auch vom Homeoffice. Ihre Rechner sind durch Kennwörter geschützt. Der Zugang zur Datenbank findet durch gesicherte VPN-Tunnel statt. Außerhalb dieser Rechner werden keine Daten gespeichert. - Passwortvergabe (Klein- und Großbuchstaben, Sonderzeichen, Zahlen, min. 8 Zeichen, regelmäßiger Wechsel) - Bildschirmsperre bei Abwesenheit mit Passwort-Aktivierung - Verbot der Nutzung privater Datenträger am Arbeitsplatz - Die Kennwörter von Bearbeitern werden als Hash mit einem Salt gespeichert. - Nur ein kleiner Kreis von Administratoren hat Zugriff auf die Datenbank - Clean Desk Policy - Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung - Rollenbezogene Rechte sind an Zugangskennungen gebunden (Einteilung nach Administrator, Benutzer etc.) - Der Zugriff und die Nutzung von Informationssystemen auf dem Server wird protokolliert, indem die Zugriffs-ID, Zugriffszeit, gewährte oder verweigerte Autorisierung und entsprechende Aktivität registriert wird, oder versetzt den Kunden dazu in die Lage. - Es werden Unterlagen über die eingehenden und ausgehenden Medien geführt einschließlich Art des Mediums, autorisierte(r)Absender/ Empfänger, Datum und Uhrzeit, Anzahl der Medien und Arten von Kundendaten, die sie enthalten.

4. Integrität	- Personen identifizierbare Eigenschaften können nur durch spezielle rollenbezogene Rechte verändert werden (Administratoren). - Protokollierung von Änderungen mit Veranlasser, Grund und Zeitpunkt. - Ein Virenschutz ist installiert und aktiviert. - Gegenseitige Überwachung (4 Augen Prinzip) - Die Kommunikation zwischen Klient und Server findet ausschließlich verschlüsselt über HTTPS statt (TLS Verschlüsselung). - Die Datenübertragung vom Auftragnehmer an den Auftraggeber kann auf unterschiedliche Arten erfolgen. Im Regelfall werden die Daten über die Kundenoberfläche zur Verfügung gestellt. Die Übertragung ist mit TLS verschlüsselt. - Direkte Verbindungen zum Servernetzwerk durch Mitarbeiter sind nur mittels VPN möglich. - Es wird sichergestellt, dass die Auftragnehmer nur mit entsprechender Verschlüsselung Daten verarbeiten oder übertragen (z.B. TLS/SSL Verschlüsselung). - Die Änderung von personenbezogenen Daten durch den Auftragsverarbeiter im Sinne von Art. 28 DSGVO erfolgt nur nach entsprechender Weisung des Auftraggebers oder der betroffenen Person selbst. - Regelmäßige Kontrolle eingesetzter Unterauftragnehmer.

5. Verfügbarkeit	- Die gesamte Serverstruktur inklusive Datenbanken wird täglich gespiegelt. - Es finden mehrmals täglich Backups der Datenbank statt. - Für den Server besteht eine unterbrechungsfreie Stromversorgung sowie weitere Systeme nach Branchenstandard, um den Verlust von Daten aufgrund von Stromversorgungsausfällen oder Leitungsstörungen zu verhindern. - Auf dem Server werden fortlaufend, jedoch keinesfalls seltener als einmal pro Woche (es sei denn, es wurden in dem Zeitraum keine Kundendaten aktualisiert) mehrere aktuelle Kopien von Kundendaten erstellt. - Datenwiederherstellungsmaßnahmen werden protokolliert, einschließlich der verantwortlichen Person, der Beschreibung der wiederhergestellten Daten, gegebenenfalls der verantwortlichen Person sowie welche Daten (gegebenenfalls) beim Datenwiederherstellungsverfahren manuell eingegeben werden mussten. - Serverseitiges BCM: PlusServer unterhält Notfallpläne für die Einrichtungen, in denen sich PlusServer-Informationssysteme, die Kunden-daten verarbeiten, befinden. Der redundante Speicher von PlusServer sowie ihre Verfahren zur Wiederherstellung von Daten sind so konzipiert, dass versucht wird, Kundendaten in ihrem ursprünglichen oder ihrem zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren. - Regelmäßige Wartung und Aktualisierung der technischen Systeme. - PlusServer verwendet Verfahren nach Branchenstandard, um Kundendaten zu löschen, wenn sie nicht mehr benötigt werden.
6. Belastbarkeit	- Für wichtige IT-Systeme werden ausreichend Ressourcen zur Verfügung gestellt.

7. Physischer oder technischer Zwischenfall	- Echtzeit Monitoring aller technischen Systeme. - Ein Virenschutz ist installiert und aktiviert. - Incident-Response-Management: Ein Ticketsystem stellt die zeitnahe Abarbeitung aller Anfragen sicher. - Die Daten der Mandanten werden getrennt verarbeitet und sind durch eindeutige Identifikationen voneinander getrennt. - Es werden Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort aufbewahrt als an dem Ort, an dem sich die primären Computergeräte, die die Kundendaten verarbeiten, befinden.
8. Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM	- Die Mitarbeiter werden 1-mal jährlich geschult und sind dazu angehalten, die Datenschutzstandards umzusetzen und weiterzuentwickeln. - Es besteht keine Pflicht zur Bestellung eines betrieblichen Datenschutz- beauftragten. Es wird zur Unterstützung bei der Umsetzung und regelmäßigen Überprüfung der datenschutzrechtlichen Pflichten, inklusive der technischen und organisatorischen Maßnahmen ein Dienstleister beauftragt. - Datenschutzvorfälle werden stets dokumentiert und ausgewertet.

Anlage 3
Vertragsergänzung für Vereinbarungen zur Auftragsverarbeitung mit kirchlichen Stellen und Organisationen

Wir bestätigen hiermit, dass unsere Vereinbarung zur Auftragsverarbeitung auch unter den Gesichtspunkten der kirchlichen Datenschutzgesetze EKD-Datenschutzgesetz (DSG-EKD 2018) und des KDG gültig ist.

Der Abschluss von Verträgen zur Auftragsverarbeitung können entsprechende Stellen auch mit Auftragsverarbeitern abschließen, auf die die kirchlichen Datenschutzbestimmungen keine Anwendung finden. Hierzu dürfen sich die Vertragsinhalte gemäß § 30 Abs. 5 DSG-EKD 2018 sowie § 29 Abs. 3 KDG an denen von Art. 28 DSGVO orientieren.

Abweichend von den allgemeinen Vorgaben im AV-Vertrag gelten für kirchliche Auftraggeber zusätzlich folgende ergänzende Regelungen:

(1) Für kirchliche Stellen und Organisationen gilt insbesondere die Zuständigkeit der jeweiligen kirchlichen Datenschutzaufsicht.

(2) Der Standort unserer Server befindet sich in Deutschland.

(3) Wir übermitteln Daten an Unternehmen in Länder außerhalb der EU nur im Einzelfall und nur auf Grundlage einer gesetzlichen Erlaubnis, wenn der Nutzer in die Übermittlung eingewilligt hat, eine rechtliche oder vertragliche Verpflichtung besteht oder wenn wir ein berechtigtes Interesse an der Übermittlung haben und das Gegenüber ein angemessenes Datenschutzniveau nach europäischen Vorgaben sicherstellt (z.B. bei Übermittlung ins außereuropäische Ausland durch Teilnahme des Unternehmens am „Privacy Shield“ oder durch Abschluss von Standardvertragsklauseln).