Vertrag über gemeinsame Verantwortlichkeit nach § 28 KDG

zwischen

dem **Bonifatiuswerk der deutschen Katholiken e.V.**, Kamp 22, 33098 Paderborn

(im Folgenden „Bonifatiuswerk“)

und

der jeweils die Firm-App für die Firmvorbereitung verwendenden Gemeinde

(im Folgenden „Gemeinde“)

(Bonifatiuswerk und Gemeinde gemeinsam im Folgenden „Parteien“ oder einzeln auch „Partei)

Präambel

Die Verwendung der Firm-App durch die Gemeinde entsprechend dem zwischen den Parteien abgeschlossenen Nutzungsvertrag bringt es mit sich, dass die Parteien gemeinsam über die Zwecke und/oder Mittel der Verarbeitung von bestimmten personenbezogenen Daten (nachfolgend auch nur "Daten" oder "Datenverarbeitung" genannt) bestimmen und im Rahmen dieser Zusammenarbeit als gemeinsame Verantwortliche nach § 28 KDG agieren. Dies vorausgeschickt, regeln die Parteien ihre datenschutzrechtlichen Rechte und Pflichten in Bezug auf die gemeinsame Verarbeitung der Daten wie folgt:

§ 1 Vertragsgegenstand

(1) Bonifatiuswerk betreibt eine Anwendung für mobile Endgeräte, die von den Nutzern im Zusammenhang der Firmvorbereitung verwendet werden soll (im Folgenden auch „Firm-App“).

(2) Die Gemeinde ist für die Durchführung der Firmung der Firmbewerber als Initiationssakrament verantwortlich. In diesem Zusammenhang setzt die Gemeinde gemäß den vertraglichen Abreden der Partei die Firm-App ein.

(3) Die Zusammenarbeit der Parteien im Hinblick auf die Verwendung der Firm-App zur Firmvorbereitung bringt es mit sich, dass die Parteien gemeinsam über die Zwecke und wesentlichen Elemente der Mittel der Verarbeitung von personenbezogenen Daten (im Folgenden auch „Verarbeitung) bestimmen und entscheiden. Aus § 28 Abs. 1 KDG folgt für diesen Fall die Pflicht, dass die Parteien miteinander eine Vereinbarung treffen, die in transparenter Form festlegt, welche Partei bestimmte Pflichten nach dem KDG und – soweit überhaupt anwendbar – der DSGVO zu erfüllen hat. Insofern dient dieser Vertrag der Erfüllung der Voraussetzungen des § 28 KDG.

§ 2 Berechtigung zum Vertragsschluss

Die für die Parteien jeweils unterzeichnenden Personen erklären, nicht im eigenen Namen, sondern für den im Rubrum bezeichneten Rechtsträger zu handeln. Sofern für die Berechtigung Beschlüsse oder Vollmachten erforderlich sind, hat die unterzeichnende Person diese im Vorhinein zu diesem Vertragsschluss eingeholt.

§ 3 Konkretisierung der Datenverarbeitung

(1) Die einzelnen Datenverarbeitungen ergeben sich aus dem zwischen den Parteien abgeschlossenen Nutzungsvertrag.

(2) Zweck der Verarbeitung ist der gemeinsame Betrieb der Firm-App mit den jeweils aktuellen Funktionalitäten der Firm-App sowie die damit verbundene elektronische Organisation und Verwaltung der Firmvorbereitung.

(3) Die Parteien stimmen überein, dass die Datenverarbeitung auf dem Gebiet der Bundesrepublik Deutschland, jedenfalls aber innerhalb der Europäischen Union, stattfindet. Jede Verlagerung in ein Drittland im Sinne des § 4 Nr. 18 KDG muss zwischen den Parteien abgestimmt werden und darf generell nur erfolgen, wenn die besonderen Voraussetzungen der §§ 39ff. KDG erfüllt sind.

§ 4 Aufteilung der Zuständigkeiten

(1) Die Parteien teilen im Folgenden die Zuständigkeiten für die nachstehend beschriebenen Datenverarbeitungsvorgänge und die Erfüllung der datenschutzrechtlichen Pflichten nach dem KDG bzw. – soweit überhaupt anwendbar – der DSGVO in diesem Zusammenhang auf.

(2) Das Bonifatiuswerk ist für Datenverarbeitungsvorgänge im Zusammenhang mit dem technischen Betrieb der Firm-App verantwortlich. Dies betrifft insbesondere die auf den für den Betrieb der Firm-App erforderlichen Servern (im Folgenden „Server“) abgelegten Informationen und Daten. Die Zuständigkeit umfasst

a. die Aktualisierung der datenschutzrechtlich relevanten Dokumente und Verträge, insbesondere der Datenschutzerklärung, der Nutzungsbedingungen und etwaigen Auftragsverarbeitungsverträgen mit Auftragnehmern des Bonifatiuswerks;

b. die Überwachung der Auftragnehmer und Unterauftragnehmer des Bonifatiuswerks im Zusammenhang mit dem Betrieb der Firm-App;

c. die Gewährleistung einer angemessenen Datensicherheit im Hinblick auf die auf den Servern abgelegten personenbezogenen Daten, insbesondere durch die Implementierung von geeigneten technischen und organisatorischen Maßnahmen im Sinne des § 26 KDG.

(3) Soweit ein Datenverarbeitungsvorgang oder eine Pflicht nach dem KDG nicht in Absatz (2) oder anderweitig in diesem Vertrag dem Bonifatiuswerk zugewiesen wurde, ist die Gemeinde zuständig. Dies betrifft insbesondere die nachstehenden Verantwortlichkeiten:

a. Das Erheben, das Einpflegen und die sonstige Verwaltung der personenbezogenen Daten der Firmbewerber und/oder Multiplikatoren und/oder Gruppenleitern und/oder sonstigen Personen im Einwirkungsbereich der Gemeinde;

b. Anlage von Benutzerkonten in der Firm-App;

c. Verwaltung von Inhalten der Firm-App im Backend der Firm-App.

(4) Ungeachtet der vorstehenden Zuständigkeiten bleiben die betroffenen Personen gegenüber jeder Partei zur Geltendmachung ihrer Rechte einzeln berechtigt. Die Parteien werden sich über Anfragen und/oder Beschwerden von Betroffenen unverzüglich informieren.

§ 5 Information über Betroffenenrechte

(1) Die datenschutzrechtlich erforderliche Information über Betroffenenrechte gegenüber den betroffenen Personen wegen Datenverarbeitungsvorgängen innerhalb der Firm-App, insbesondere aus §§ 14, 15 KDG, wird durch das Bonifatiuswerk sichergestellt.

(2) Betroffenen Personen sind die erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung zu stellen. Die Parteien werden sich auf Inhalt und Formulierung dieser Informationen verständigen.

(3) Das Bonifatiuswerk wird die betroffenen Personen im Wege der Informationserteilung über Betroffenenrechte ebenfalls über die wesentlichen Inhalte dieser Vereinbarung aufklären.

(4) Die Information über Betroffenenrechte wird das Bonifatiuswerk zum Abruf in der Firm-App bereitstellen.

(5) Über Betroffenenrechte im Zusammenhang mit Verarbeitungsvorgängen, die nicht im Zusammenhang mit dem Betrieb der Firm-App stehen, wird die Gemeinde die betroffenen Personen informieren.

§ 6 Datensicherheit

(1) Die Parteien ergreifen in ihrem jeweiligen Zuständigkeitsbereich nach § 4 zur Gewährleistung der Sicherheit der verarbeiteten personenbezogenen Daten technische und organisatorische Maßnahmen, die den Voraussetzungen des § 26 KDG entsprechen und geeignet sind, die Datensicherheit herzustellen.

(2) Die nachstehenden technischen und organisatorischen Maßnahmen sehen die Parteien als geeignet an:

a. **Zutrittskontrolle**, d.h. Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, nämlich insbesondere durch

   i. Gebäudesicherung wie Sicherheitsschlösser, Schließen und Alarmanlagen;
   ii. Sicherung der Datenverarbeitungsanlagen, wie in Form von verschließbaren Server- und Aktenschränken
   iii. Schlüsselregelungen und -management;
   iv. Zugangsgewährung nur für Mitarbeiter und Reinigungsdienste sowie die Gewährleistung einer ständigen Begleitung von Gästen durch einen Mitarbeiter;
   v. Sicherstellung der uneinsehbaren Aufbewahrung, bei körperlich vorhandenen Daten etwa durch die Aufbewahrung in fensterlosen Räumen/vor dem Blick von außen geschützten Behältnissen;
   vi. Aufbewahrung von Notebooks und Datenträgern in abgeschlossenen Räumen;
   vii. Absicherung der Gebäudeschächte und sorgfältiger Auswahl der Reinigungsdienste.

b. **Zugangskontrolle**, d.h. Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können, nämlich insbesondere durch

   i. Login mit Benutzername und Passwort;
   ii. Einrichten einer Passwort-Richtlinie (insbesondere zur regelmäßigen Änderung sowie Mindestanzahl an verschiedenen Zeichen);
   iii. Verwalten von Benutzerberechtigungen;
   iv. Einsatz von Antiviren Software;
   v. Zentrale Passwortvergabe;
   vi. Firewalls;
   vii. Richtlinie Clean Desk;
   viii. Policy für mobile Geräte;
   ix. Verschlüsselung von Datenträgern und Notebooks/Tablets.

c. **Zugriffskontrolle**, d.h. Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, nämlich insbesondere durch

   i. Aktenvernichter oder vergleichbares;
   ii. Einsatzberechtigungskonzepte;
   iii. physische Löschung und Überschreibung von Datenträgern;
   iv. Beschränkung der Anzahl von Administratoren auf das „Notwendige“;
   v. Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten;
   vi. Verwaltung der Benutzerrechte durch minimale Anzahl von Administratoren.

d. **Trennungskontrolle**, d.h. Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, nämlich insbesondere durch

   i. Berechtigungskonzept;
   ii. Physikalische Trennung (Systeme/Datenbanken/Datenträger);
   iii. Festlegung von Datenbankrechten;
   iv. Mandantenfähigkeit relevanter Anwendungen.

e. **Pseudonymisierung**, d.h. die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

f. **Weitergabekontrolle**, d.h. Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder

während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist, etwa durch

i. E-Mail-Verschlüsselung;
ii. Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. Löschfristen;
iii. Bereitstellung über verschlüsselte Verbindungen wie SFTP, SSL-Verschlüsselung (https).

g. **Eingabekontrolle**, d.h. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, etwa durch

i. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzer-gruppen) und technische Protokolle;
ii. Klare Zugriffsberechtigungen und Zuständigkeiten für Löschungen.

h. **Verfügbarkeitskontrolle**, d.h. Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, etwa durch

i. Feuer- und Rauchmeldeanlagen;
ii. Backup & Recovery-Konzept;
iii. Feuerlöscher;
iv. Regelmäßig Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse;
v. Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums;
vi. Keine sanitären Anschlüsse in Nähe des Serverraums oder Datenverarbeitungsgeräten.

i. **Datenschutz-Management**, etwa durch

   i. Dokumentation zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung;
   ii. Verpflichtung der Mitarbeiter auf Vertraulichkeit/Datengeheimnis;
   iii. Einen internen oder Informationssicherheits- und Datenschutzbeauftragten
   iv. Informationspflichten hinsichtlich Datenverarbeitung nach §§ 14 bis 16 KDG und Art. 13 und 14 DSGVO
   v. Einsatz von Firewall und regelmäßiger Aktualisierung;
   vi. Dokumentierten Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde);
   vii. Einsatz von Spamfiltern regelmäßiger Aktualisierung;
   viii. Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen (Notfallplan);
   ix. Einsatz von Virenscanner und regelmäßiger Aktualisierung

j. **Auftragskontrolle**, d.h. Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können, etwa durch

   i. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit);
   ii. Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln;
   iii. Schriftliche Weisungen an den Auftragnehmer;
   iv. Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis;
   v. Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer;
   vi. Regelung zum Einsatz weiterer Subunternehmer;
   vii. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags;

viii. Bei längerer Zusammenarbeit: laufende Überprüfung des Auftragnehmers und seines Schutzniveaus.

§ 7 Umgang mit Datenschutzverletzungen und Datenschutzvorfällen

(1) Für die Prüfung und Bearbeitung aller Verletzungen des Schutzes personenbezogener Daten, einschließlich der Erfüllung deshalb bestehender Meldepflichten gegenüber der zuständigen Aufsichtsbehörde bzw. den Betroffenen ist das Bonifatiuswerk zuständig. Die Gemeinde wird das Bonifatiuswerk bestmöglich unterstützen und etwaig erforderliche Unterlagen und Informationen bereitstellen. In Abstimmung der Parteien kann die Prüfung und Bearbeitung auch durch den betrieblichen Datenschutzbeauftragten des Bistums oder der Gemeinde erfolgen.

(2) Wird einer der Parteien eine Verletzung des Datenschutzes bekannt oder tritt eine sicherheitsrelevante Störung des Datenverarbeitungsprozesses auf, sind die Parteien ungeachtet der Zuständigkeitsverteilung verpflichtet, innerhalb ihrer Organisation unverzüglich Maßnahmen zu ergreifen, die zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen erforderlich sind. Der Vorfall ist der jeweils anderen Partei unverzüglich zu melden.

(3) Ungeachtet der Zuständigkeitsverteilung gemäß § 4 dieses Vertrages werden die Parteien der jeweils anderen Partei unverzüglich anzeigen, wenn sich eine Datenschutzaufsicht im Zusammenhang mit diesem Vertrag an sie wendet. Die Parteien stimmen darin überein, dass sie den Aufforderungen zuständiger Datenschutzaufsicht grundsätzlich Folge leisten werden, insbesondere in Bezug auf Anfragen und die Überlassung von Informationen.

(4) Bevor eine Meldung an die Datenschutzaufsicht erfolgt oder einer Anfrage einer Datenschutzaufsicht Folge geleistet wird, werden sich die Parteien hinsichtlich des Vorgehens abstimmen.

§ 8 Einschalten von Auftragsverarbeitern

(1) Die Parteien dürfen Auftragsverarbeiter im Sinne von § 4 Nr. 10 KDG nur für die ihnen nach § 4 dieses Vertrags jeweils zugewiesenen Aufgaben und nur nach

vorheriger schriftlicher Zustimmung der anderen Partei einschalten. Dies gilt nicht für die nachstehenden Auftragsverarbeiter des Bonifatiuswerk, denen die Gemeinde hiermit zustimmt:

Tellux Next GmbH, Laplacestr. 12, 81679 München für den technischen Betrieb der Firm-App sowie den nachstehenden Unterauftragnehmer der Tellux Next GmbH:

a. Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg;
b. Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland als Anbieter von “Firebase Cloud Messaging”;
c. Netlify Inc, 44 Montgomery Street, Suite 300, San Francisco, Kalifornien 94104, USA
d. Maconit Consulting GmbH, Riedstraße 6, 82178 Puchheim;
e. QM Interactive GmbH, Thierschstr. 34, 80538 München.

(2) Die Einschaltung von Auftragsverarbeitern erfolgt durch schriftliche Vereinbarung, die den Anforderungen der § 29 KDG entsprechen muss.

(3) Jede Partei prüft ihre Auftragsverarbeiter regelmäßig in geeigneter Form.

§ 9 Sonstige gemeinsame und gegenseitige Pflichten

(1) Die Parteien werden alle mit der Datenverarbeitung beschäftigten Personen schriftlich zur Vertraulichkeit im Hinblick auf die Daten verpflichten.

(2) Die Parteien führen ein Verzeichnis zu allen Kategorien von in gemeinsamer Verantwortlichkeit durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben nach § 31 KDG enthält.

(3) Sofern und solange die gesetzlichen Voraussetzungen gegeben sind, werden die Parteien jeweils einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten gemäß §§ 36ff. KDG bestellen.

§ 10 Schlussbestimmungen

(1) Dieser Vertrag ist an die Laufzeit und Beendigung des Nutzungsvertrags gekoppelt. Dieser Vertrag kann nicht losgelöst von dem Nutzungsvertrag beendet werden. Dieser Vertrag steht unter der auflösenden Bedingung der Beendigung des Nutzungsvertrags über die Firm-App.

(2) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam erweisen oder eine Lücke enthalten, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt. An die Stelle der unwirksamen Regelung soll eine gesetzlich zulässige Regelung treten, die dem Sinn und Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des § 28 KDG entspricht.