**Zusatzvereinbarung nach § 8 KDO bzw. § 11 BDSG**

**zur**

**"Datenverarbeitung im Auftrag"**

zwischen

**dem Erzbistum Köln, KdöR, vertreten durch den Generalvikar Dr. Dominik Meiering, Marzellenstr. 32, 50606 Köln**

(nachstehend Auftraggeber genannt)

und

**QuestMill GmbH, vertreten durch den Geschäftsführer Holger Mügge**

**Clostermannstr. 1, 51065 Köln**

(nachstehend Auftragnehmer genannt)

# Gegenstand des zugrundeliegenden Auftrags

Auftraggeber und Auftragnehmer haben mit dem zeitgleich abgeschlossenen Software-Lizenzvertrag (nachstehend Leistungsvereinbarung) eine Vereinbarung getroffen über den zeitlich befristeten Einsatz der von QuestMill entwickelten Software „GeoQuest“ für Nutzer des (Web-)Angebots [www.tap-erlebnis.de](http://www.tap-erlebnis.de).

# Weisungsbefugnis des Auftraggebers

Der Umgang mit den personenbezogenen Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (§ 8 Abs. 3 KDO bzw. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Mündliche Weisungen wird der Auftraggeber unverzüglich in Textform bestätigen.

Die Weisungsberechtigten des Auftraggebers sind in Anlage 1 aufgeführt.

# Befugnisse des Auftragnehmers im Umgang mit den Daten des Auftraggebers

Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer sind in der Leistungsvereinbarung beschrieben [alternativ: Nennung von Umfang, Art und Zweck]. Diese Beschreibung ist abschließend.

Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Änderungen, Löschungen oder Sperrungen von Daten darf der Auftragnehmer nur nach Weisung des Auftraggebers vornehmen.

Auskünfte an Betroffene oder Dritte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Die Verarbeitung und Nutzung der Daten findet ausschließlich in Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in einen anderen Staat bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen nach §§ 4b, 4c BDSG erfüllt sind.

# Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer hat zu gewährleisten, dass die Anforderungen zum Schutz der personen­bezogenen Daten eingehalten werden. Die erforderlichen technischen und organisatorischen Maßnahmen (nachstehend TOM) nach § 6 KDO und Anlage (KDO-DVO) bzw. § 9 BDSG und Anlage sind in Anlage 2 zu dieser Zusatzvereinbarung dargestellt.

Der Auftragnehmer hat die Umsetzung der TOM hinsichtlich der konkreten Durchführung des Auftrags vor Beginn der Verarbeitung zu dokumentieren. Als Nachweis der unabhängig vom Auftrag generell getroffenen technischen und organisatorischen Maßnahmen gegen­über dem Auftraggeber kann der Auftragnehmer aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) verwenden.

Die Dokumentation ist auf Verlangen dem Auftraggeber zur Prüfung zu übergeben. Soweit die Prüfung durch den Auftraggeber einen Anpassungsbedarf ergibt, wird dieser nach Absprache realisiert.

Die vom Auftragnehmer dokumentierten und von Auftraggeber akzeptierten Maßnahmen sind Grundlage und Bestandteil des zugrundeliegenden Auftragsverhältnisses.

Die Anforderungen an die technischen und organisatorischen Maßnahmen sowie ihre Realisierung unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern mit den neuen Maßnahmen das Sicherheitsniveau der vereinbarten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind vom Auftragnehmer zu dokumentieren.

Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

# Weitere Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich folgende Pflichten:

* Wahrung des Datengeheimnisses (§ 4 KDO bzw. § 5 BDSG): Alle Personen, die im Rahmen des Auftrags auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis durch Unterschrift verpflichtet sein und über die sich aus dem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt worden sein.
* Unverzügliche Information des Auftraggebers, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften (§ 8 Abs. 3 S. 2 KDO bzw. § 11 Abs. 3 Satz 2 BDSG). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
* Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
* Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten (§§ 4f, 4g BDSG). Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
* Unverzügliche Weiterleitung an den Auftraggeber, wenn ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Änderung, Löschung oder Sperrung seiner Daten wendet.
* Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach §§ 38, 43 oder 44 BDSG.

# Unterauftragsverhältnisse

Die Einbeziehung von Unterauftragnehmern bei der Verarbeitung oder Nutzung personen­bezogener Daten des Auftraggebers ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet.

Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner in Abschnitt 4 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn des Einsatzes mitteilt.

Der Auftragnehmer hat die vertraglichen Vereinbarungen mit Unterauftragnehmern so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte ent­sprechend dieser Vereinbarung und gemäß § 8 KDO bzw. § 11 und Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftrag­gebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesent­lichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unter­auf­tragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertrags­unterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Leistungen in den Bereichen Telekommunikation, IT-Service, Reinigung, Entsorgung und Prüfung. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzes­konforme vertragliche Vereinbarungen zu treffen sowie die Durchführung der vereinbarten Maßnahmen zu kontrollieren.

# Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die Auftragskontrolle (Nr. 6 der Anlage zu § 6 KDO bzw. Nr. 6 der Anlage zu § 9 BDSG) in Abstimmung mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags (§ 8 Abs. 2 Satz 3 KDO bzw. § 11 Abs. 2 Satz 4 BDSG) stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

# Maßnahmen bei Verstößen gegen den Datenschutz

Wenn durch den Auftragnehmer oder eine bei ihm beschäftigte oder beauftragte Person ein Verstoß gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag oder in dieser Vereinbarung getroffenen datenschutzrechtlichen Festlegungen vorgefallen ist sowie bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers ist der Auftragnehmer unverzüglich zu folgenden Maßnahmen verpflichtet:

* Meldung an den Auftraggeber ohne Ansehen von Verursachung oder Verschulden
* angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene
* Absprache mit dem Auftraggeber über weitere Maßnahmen
* Unterstützung des Auftraggebers im Zusammenhang mit Verpflichtungen nach § 42a BDSG

# Rückgabe bzw. Löschung von Datenbeständen

Nach Abschluss der vertraglichen Tätigkeiten oder früher nach Aufforderung durch den Auftrag­geber, spätestens mit Ablauf der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinem Besitz befindlichen Unterlagen, Verarbeitungs- und Nutzungs­ergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, einschließlich aller Datensicherungen dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung (Muster in Anlage 3) ist dem Auftraggeber vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

# Laufzeit der Zusatzvereinbarung

Die Geltung dieser Zusatzvereinbarung endet mit der Geltung der Leistungsvereinbarung.

Die Verpflichtung des Auftragnehmers zur Verschwiegenheit besteht über die Geltung der Zusatzvereinbarung hinaus auf unbeschränkte Zeit (§ 4 Satz 3 KDO bzw. § 5 Satz 3 BDSG).

# Schlussbestimmungen

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder sich nach Abschluss der Vereinbarung als unwirksam oder undurchführbar erweisen, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkung der datenschutzrechtlichen Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Dies gilt entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Auftragnehmer Auftraggeber

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum Unterschrift Datum Unterschrift

**Anlage 1:**

**Weisungsberechtige Personen und Weisungsempfänger**

**Weisungsempfänger beim Auftragnehmer:**

* Verantwortlicher: Holger Mügge
* AP/Verantwortlicher IT: Kevin Glaap
* ggf. IT-Sicherheitsbeauftragter, Informationssicherheitsbeauftragter: Holger Mügge
* alle Mitarbeitenden im involvierten Team: Holger Mügge, Kevin Glaap, Carlos Cervantes

**Datenschutzbeauftragter des Auftragnehmers:**

* Herr Holger Mügge

**Weisungsberechtigte Personen des Auftraggebers:**

* AP Fachbereich: Efi Goebel
* ggf. weitere APs: Ursula Pies-Brodesser, Dr. Holger Dörnemann
* Herr Dirk Hennemann, Zentraler Informationssicherheitsbeauftragter

**Datenschutzbeauftragte des Auftraggebers:**

* Frau Dr. Susanne Eberle, Diözesandatenschutzbeauftragte
* Herr Peter Heidkamp, Betrieblicher Datenschutzbeauftragter des EGV

Beide Vertragsparteien stellen für die genannten Personen eine Verhinderungsvertretung sicher. Ein Wechsel einer der genannten Personen wird der jeweils anderen Vertragspartei unverzüglich mitgeteilt.

Auftragnehmer Auftraggeber

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum Unterschrift Datum Unterschrift

**Anlage 2:**

**Technische und organisatorische Maßnahmen nach § 6 KDO und Anlage   
(bzw. § 9 BDSG und Anlage)**

1. **Technische Maßnahmen**
   1. **Zutrittskontrolle**

*Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.*

Maßnahmen zur Legitimation der Berechtigten (Beispiele):

* Zutrittskontrollsystem, z. B. Ausweisleser, Magnetkarte, Chipkarte (zu beachten: § 5b KDO bzw. § 6c BDSG)
* Türsicherung (elektrische Türöffner usw.)
* Einsatz von Werkschutz, Pförtner, etc.
* Einsatz von Überwachungseinrichtungen, z. B. Alarmanlage, optische Monitore (zu beachten: § 5a KDO bzw. § 6b BDSG)
  1. **Zugangskontrolle**

*Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.*

Maßnahmen zur Identifizierung und Authentifizierung der Benutzer (Beispiele):

* Einrichtung eines Benutzerstammsatzes pro User
* Qualifizierung der Kennworte (z. B. Mindestlänge, Sonderzeichen, regelmäßiger Wechsel des Kennworts)
* Automatische Sperrung nach einer Zeit der Nichtnutzung
  1. **Zugriffskontrolle**

*Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.*

Maßnahmen zur restriktiven Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung (Beispiele):

* Einrichtung differenzierter Berechtigungen (Rollen, Transaktionen und Objekte)
* Auswertungen über die Nutzung von Berechtigungen
* unverzügliche Löschung nicht mehr erforderlicher Berechtigungen
  1. **Weitergabekontrolle**

*Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ...*

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung (Beispiele):

* Verschlüsselung von Datenträgern
* Verschlüsselung von Datenverbindungen
* Elektronische Signatur
* Protokollierung des Datenverkehrs
* Transportsicherung
  1. **Eingabekontrolle**

*Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.*

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind (Beispiele):

* Benutzeridentifikation
* Protokollierungssysteme
* Protokollauswertungssysteme
  1. **Auftragskontrolle**

*Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.*

Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer (Beispiele):

* Eindeutige Vertragsgestaltung
* Kriterien zur Auswahl des Auftragnehmers
* Kontrolle der Vertragsausführung
  1. **Verfügbarkeitskontrolle**

*Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.*

Maßnahmen zur physikalischen und logischen Datensicherung (Beispiele):

* Spiegelung von Festplatten
* Unterbrechungsfreie Stromversorgung (USV)
* Virenschutz / Firewall
* Backup-Verfahren
* Getrennte Aufbewahrung von Datensicherungen
* Notfallplan
  1. **Trennungsgebot**

*Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.*

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken (Beispiele):

* Funktionstrennung zwischen Test und Produktion
* Mandantenfähigkeit der Systeme

1. **Organisatorische Maßnahmen**

Organisatorische Maßnahmen bestehen in der Regel aus Prozess-Anweisungen sowie der Kontrolle ihrer Realisierung, z. B.:

* Verfahren zur Ausgabe von Schlüsseln
* Verfahren zur Besucheranmeldung
* Einhaltung eines Vier-Augen-Prinzips
* Durchführung von Stichprobenprüfungen in festgelegten Intervallen
* Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen

**Anlage 3:**

**Bestätigung der Löschung bzw. Vernichtung von Daten des Erzbistums**

Diese Bestätigung gilt für sämtliche Daten, die ausschließlich zur Bearbeitung im Rahmen des Projektes [Projektname, alternativ: kurze Zweckbeschreibung] an den Auftragnehmer übermittelt wurden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | erfolgt | nicht erfolgt | nicht relevant |
| Sämtliche permanenten Datenträger wie CDs, DVDs o. ä. sind an den Auftraggeber zurückgesandt. |  | □ | □ | □ |
| Sämtliche flüchtigen Datenträger wie USB-Sticks, Memory-Cards o. ä. sind an den Auftraggeber zurückgesandt. |  | □ | □ | □ |
| Sämtliche flüchtigen Datenträger wie USB-Sticks, Memory-Cards o. ä. sind nachhaltig gelöscht. |  | □ | □ | □ |
| Sämtliche weiteren Datenträger (auch in Papierform) sind vernichtet und der Nachweis hierüber ist an den Auftraggeber zurückgesandt. |  | □ | □ | □ |
|  |  |  |  |  |
| Sämtliche Daten in Dateiform auf internen Systemen inkl. aller Kopien sind gelöscht. |  | □ | □ | □ |
| Sämtliche Daten, die ausschließlich im Rahmen des betreffenden Auftrages in internen Anwendungen bzw. Datenbanken gespeichert wurden, sind gelöscht. |  | □ | □ | □ |
| Sämtliche Kopien von Daten, die im Rahmen von Datensicherungsroutinen erstellt wurden, sind gelöscht. |  | □ | □ | □ |

Auftragnehmer

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum Unterschrift