Auftragsbearbeitungsvertrag

zwischen

_____

als Verantwortlicher (nachfolgend „**Verantwortlicher**“),

und

XQueue GmbH, Christian-Pleß-Straße 11-13, 63069 Offenbach am Main, Deutschland

als Auftragnehmer (nachfolgend „**Auftragnehmer**“,
Verantwortlicher und Auftragnehmer gemeinsam die “**Parteien**”)

Präambel

Der Verantwortliche hat den Auftragnehmer im bereits geschlossenen Vertrag (nachfolgend „**Hauptvertrag**“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Bearbeitung von Personendaten. Insbesondere Art. 9 Schweizer Bundesgesetz über den Datenschutz (nachfolgend “**DSG**”) und Art. 28 EU-Datenschutz-Grundverordnung (nachfolgend nur “**DSGVO**”) stellen bestimmte Anforderungen an eine solche Auftragsbearbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsbearbeitungsvertrag (nachfolgend die “**Vereinbarung**”), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 5 lit. j DSG und 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Bearbeitung von Personendaten entscheidet.

(2) Auftragnehmer ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personendaten im Auftrag des Verantwortlichen bearbeitet. In Art. 5 lit. k DSG wird der Auftragnehmer als Auftragsbearbeiter und in Art. 4 Abs. 8 DSGVO Auftragsverarbeiter genannt.

(3) Personendaten sind gem. Art. 5 lit. a DSG und 4 Abs. 1 DSGVO (dort “personenbezogene Daten”

genannt) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (nachfolgend „**Betroffener**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Bearbeitung ist gem. 5 lit. d DSG und 4 Abs. 2 DSGVO (dort “Verarbeitung” genannt) jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personendaten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 1 DSG der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) für die Schweiz und gem. Art. 4 Abs. 21 DSGVO eine von einem EU-Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle für die EU.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Verantwortlichen die im Hauptvertrag genannten Leistungen. Dabei erhält der Auftragnehmer Zugriff auf Personendaten, die der Auftragnehmer für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen bearbeitet. Umfang und Zweck der Datenbearbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenbearbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit Personendaten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, bearbeiten oder nutzen. Wird der Auftragnehmer durch das Recht der Schweiz, der Europäischen Union oder der EU-Mitgliedstaaten, soweit er diesem unterliegt, zu weiteren Bearbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Bearbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch den Hauptvertrag sowie diese Vereinbarung festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die vereinbarte Leistung des Hauptvertrags hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der bearbeiteten Daten, Kreis der Betroffenen, Drittland

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten Personendaten.

(2) Der Kreis der von der Datenbearbeitung Betroffenen ist in **Anlage 2** dargestellt.

(3) Eine Weitergabe von Personendaten darf

- im Anwendungsbereich des DSG von der Schweiz in ein Land außerhalb der Schweiz nur unter den Voraussetzungen der Art. 16 ff. DSG
- im Anwendungsbereich der DSGVO aus dem Europäischen Wirtschaftsraum in ein Land außerhalb nur unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 3** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 8 DSG und Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenbearbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, Personendaten unbefugt zu erheben, zu bearbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend "**Mitarbeiter**"), entsprechend verpflichtenund mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

(4) Der Auftragnehmer hat einen Datenschutzberater oder Datenschutzbeauftragten benannt. Der Datenschutzberater oder Datenschutzbeauftragte des Auftragnehmers ist heyData GmbH, Schützenstr. 5, 10117 Berlin, Deutschland, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Bearbeitung der Personendaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes von Personendaten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes von Personendaten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen Personendatensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes von Personendaten.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenbearbeitung und sodann jährlich von den technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen. Ein Recht auf eine bestimmte Art von Auskunft oder einen bestimmten Nachweis besteht nicht. Es steht dem Auftragnehmer frei, angefragte Auskünfte oder Nachweise durch andere zu ersetzen.

(2) Der Verantwortliche darf die technischen und organisatorischen Maßnahmen des Auftragnehmers in begründeten Fällen nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Ein begründeter Fall im Sinne des § 7 Abs. 2 S. 1 liegt nur vor, wenn der Verantwortliche konkrete Nachweise vorlegt, nach denen der Auftragnehmer die Anforderungen dieser Vereinbarung nicht einhält.

(3) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Einsatz von Dienstleistern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 4** genannten Dienstleister (nachfolgend "**UnterAuftragnehmer**") durchgeführt. Der Verantwortliche erteilt dem Auftragnehmer seine allgemeine Genehmigung im Sinne von Art. 9 Abs. 3 DSG und Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere UnterAuftragnehmer zu beauftragen oder bereits beauftragte zu ersetzen.

(2) Der Auftragnehmer wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines UnterAuftragnehmers informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines UnterAuftragnehmers aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

(3) Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines UnterAuftragnehmers ist innerhalb von 2 Wochen nach Erhalt der Information über die Änderung zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragnehmer nicht möglich, steht dem Auftragnehmer ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

(4) Der Auftragnehmer hat bei der Einschaltung von UnterAuftragnehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

(5) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 19, 21, 22, 24, 25 und 28 DSG und Art. 12–22 sowie 32 bis 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung

hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenbearbeitung oder Nutzung im Rahmen der Auftragsbearbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer allein der Verantwortliche gegenüber dem Betroffenen verantwortlich.

(2) Der Auftragnehmer haftet für Schäden unbeschränkt, soweit die Schadensursache auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Auftragnehmers, seines gesetzlichen Vertreters oder Erfüllungsgehilfen beruht.

(3) Für fahrlässiges Verhalten haftet der Auftragnehmer nur bei Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Verantwortliche regelmäßig vertraut und vertrauen darf, jedoch beschränkt auf den vertragstypischen Durchschnittsschaden. Im Übrigen ist die Haftung des Auftragnehmers - auch für seine Erfüllungs- und Verrichtungsgehilfen - ausgeschlossen.

(4) Die Haftungsbegrenzung gemäß § 10.3 gilt nicht für Schadensersatzansprüche aus der Verletzung von Leben, Körper, Gesundheit oder aus der Übernahme einer Garantie.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach Recht der Schweiz, der Europäischen Union oder eines EU-Mitgliedstaat, soweit er diesem unterliegt, eine Verpflichtung zur Speicherung der Personendaten besteht – löschen..

(2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über Personendaten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

(1) Soweit der Auftragnehmer Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragnehmers haben diese Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon

unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt dem Recht des Staates, indem der Auftragnehmer seinen Sitz hat.

Verantwortlicher

Name: _____

Position: _____

Datum: _____

Unterschrift: _____

Auftragnehmer

Name: _____

Position: _____

Datum: _____

Unterschrift: _____

Anlagen

Anlage 1 – Beschreibung der Daten/Datenkategorien

Folgende Arten von Daten / Datenkategorien werden berarbeitet:

☐ Personenstammdaten (z.B. Anrede, Vorname, Nachname)

☐ Kommunikationsdaten (z.B. E-Mail Adresse, Telefonnummer)

☐ Adressdaten

☐ Nutzungsdaten (z.B. Einzelnutzer-Tracking)

☐ Weitere Profildaten (z.B. Alter, Schuhgröße)

☐ Vertragsstammdaten (Vertragsbeziehung, Produktinteresse)

☐ Kundenhistorie (z.B. Waren im Warenorb)

☐ Abrechnungsdaten / Zahldaten

☐ Planungs- und Steuerungsdaten (z.B. Verifizierung der erfolgten Datenübermittlung)

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien oder öffentliche Verzeichnisse)

_____

_____

_____

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Folgende Personen / Personengruppen sind von der Datenbearbeitung betroffen:

☐ Kunden

☐ Interessenten

☐ Newsletter-Empfänger / Abonnenten

☐ Nutzer des Online Shops

☐ Registrierte Nutzer des Online-Angebots / der Unternehmens-Webseite

☐ Beschäftigte

☐ Lieferanten

☐ Handelsvertreter

☐ Ansprechpartner

_____

_____

_____

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Maßnahmen zur Datenschutzkontrolle gemäß Art. 32 DS-GVO

1. Einleitung

Diese Anlage fasst die vom Auftragsverarbeitern getroffenen technische und organisatorische Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Auftragsverarbeiter personenbezogene Daten schützt. Das Dokument hat den Zweck, den Auftragsverarbeiter bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu unterstützen.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Absicherung von Gebäudeschächten
- Chipkarten-/Transponder-Schließsystem
- Videoüberwachung der Zugänge
- Protokollierung der Besucher (z.B. Besucherbuch)
- Schlüsselregelung / Schlüsselbuch
- Tragepflicht von Mitarbeiter- und Gästeausweisen
- Besucher nur in Begleitung durch Mitarbeiter
- Sorgfältige Auswahl des Reinigungspersonals

2.2 Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie bei Remote-Zugriffen
- Sperren externer Schnittstellen (z.B. USB-Anschlüsse)
- Verschlüsselung von Datenträgern

- Automatische Desktopsperre
- Verwaltung von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortregeln
- Protokollierung der Besucher (z.B. Besucherbuch)
- Schlüsselregelung / Schlüsselbuch
- Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit
- Unternehmens-Richtlinie für sichere Passwörter
- Unternehmens-Richtlinie "Löschen/Vernichten"
- Unternehmens-Richtlinie zur Verwendung mobiler Geräte
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren

2.3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Einsatz von Aktenvernichtern (mit cross cut-Funktion)
- Vernichtung von Datenträgern mindestens nach DIN 32757
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten)
- Einsatz eines Berechtigungskonzepts
- Anzahl der Administratoren ist so klein wie möglich gehalten
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren

2.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

2.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise sicher, dass sie 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. Hierzu werden die Daten vor der Weiterverarbeitung mit eindeutigen Pseudonymen verknüpft und weitere

personenbezogene Daten entfernt. Folgende Maßnahmen sind implementiert:

- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Protokollierung von Zugriffen und Abrufen
- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS
- Nutzung von Signaturverfahren
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Uploadverbot dienstlicher Daten auf unternehmensfremde Server

3.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatische Kontrolle der Protokolle
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Feuer- und Rauchmeldeanlagen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräume
- Unterbrechungsfreie Stromversorgung (USV)
- Videoüberwachung in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Regelmäßige Backups
- Keine sanitären Anlagen im oder oberhalb des Serverraums

- Trennung von Betriebssystemen und Daten

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Verwendung der heyData-Plattform zum Datenschutz-Management
- Bestellung des Datenschutzbeauftragten heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

5.2. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls

5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung:

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

5.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage

entsprechender Bestätigungen

- Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)
- Sorgfältige Auswahl von Auftragnehmern (insbesondere hinsichtlich Datensicherheit)

Anlage 4 – Aktuelle Subunternehmer

Folgende Auftragsverarbeiter wurden von XQueue GmbH beauftragt, um Informationen aus diesem Auftragsverhältnis zu verarbeiten.

Name	**Funktion**	**Serverstandort**
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Dublin, D04e5w5, Irland	serverlose Rechenumgebungen, Platform-as-a-Service und Infrastruktur-as-a-Service	EU
Hetzner Online GmbH Rechenzentrum Nürnberg	• Rechenzentrum/Cloud • Hosting Services	Industriestr. 25 91710 Gunzenhausen