Vertrag zur Auftragsverarbeitung i.S.d. Art. 28 Datenschutz Grundverordnung (DS-GVO)

zwischen dem Auftraggeber / der Auftraggeberin:

Firmenname: _____

Firmenanschrift : _____

im Folgenden auch "**Verantwortlicher**" genannt, und der

Auftragnehmerin:

XQueue GmbH
Christian-Pless-Str. 11-13, 63069 Offenbach am Main im Folgenden auch

"**Auftragsverarbeiter**" genannt.

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im bereits geschlossenen Vertrag (nachfolgend „**Hauptvertrag**“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die “**Vereinbarung**”), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gemäß Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gemäß Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gemäß Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „**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) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gemäß Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die

Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gemäß Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gemäß Art. 4 Abs. 13 DSGVO, biometrischen Daten gemäß Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gemäß Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gemäß Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gemäß Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gemäß Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

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

(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 Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten 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 darüberhinaus gehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag 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) Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

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

Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der verarbeiteten Daten, Kreis der Betroffenen

Umfang, Art und Zweck der Datenverarbeitung beschränken sich auf die Nutzung von Adressdaten zur Versendung von Newslettern per E-Mail.

Gegenstand der Verarbeitung personenbezogener Daten sind Kundendaten vom Verantwortlichen.

Die durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen sind Kunden, Geschäftskontakte und Interessenten vom Verantwortlichen.

Die verarbeiteten Arten von Daten sowie die Kategorien betroffener Personen ergeben sich aus § 12 dieses Vertrages.

§ 5 Schutzmaßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter 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 Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 1** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gemäß Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend "**Mitarbeiter**"), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragsverarbeiter bestehen bleiben.

§ 6 Informationspflichten des Auftragsverarbeiters

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach dem Vorfall oder der Unregelmäßigkeit, informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragsverarbeiter 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 personenbezogener Daten.

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

(4) Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragsverarbeiter wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Verantwortlichen liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten.

(6) An der Erstellung des Verfahrensverzeichnisses durch den Verantwortlichen hat der Auftragsverarbeiter im angemessenen Umfang mitzuwirken. Er hat dem Verantwortlichen die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig quartalsweise von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

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

(4) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragsverarbeiter weist dem Verantwortlichen die Verpflichtung der Mitarbeiter nach § 5 Abs. 3 auf Verlangen nach.

(6) Der Verantwortliche hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Verantwortlichen ist

heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 8 Einsatz von Dienstleistern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 2** genannten Dienstleister (nachfolgend "**Unterauftragsverarbeiter**") durchgeführt.

Weitere Unterauftragsverarbeiter beauftragt der Auftragsverarbeiter nur nach schriftlicher Zustimmung des Verantwortlichen.

(2) Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben. Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters 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 Auftragsverarbeiter nicht möglich, steht dem Auftragsverarbeiter ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

(3) Der Auftragsverarbeiter ist verpflichtet, Unterauftragsverabeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverabeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten. Sofern eine Einbeziehung von Unterauftragsverabeitern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass beim jeweiligen Unterauftragsverabeiter ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln mit zusätzlichen Garantien, dass das Datenschutzniveau im Drittland dem der EU entspricht). Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragsverabeitern nachweisen.

(4) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter 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 Auftragsverarbeiter 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 Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach 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 Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

§ 10 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu

kontrollieren.

(3) Der Auftragsverarbeiter 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 Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 11 Schlussbestimmungen

(1) Der Auftragsverarbeiter kann sich in Bezug auf die im Rahmen dieser Vereinbarung zu verarbeitenden Daten und die entsprechenden Datenträger nicht auf ein Zurückbehaltungsrecht gemäß § 273 des Bürgerlichen Gesetzbuches oder anderer anwendbarer Gesetze berufen.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. 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 deutschem Recht.

§ 12 Daten

Die folgenden Arten von **personenbezogenen Daten** werden im Rahmen dieser Vereinbarung verarbeitet.

Arten von Daten:

Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (geschäftlich), Rechnungsanschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Position, Kontaktdaten, Kontakthistorie, Vertragsdaten

Darüber hinaus sind die folgenden **Kategorien von Personen** betroffen.

Verantwortlicher, Kunden des Verantwortlichen, Dritte

Anlage 1: Datensicherheitskonzept

Anlage 2: Unterauftragnehmer

Verantwortlicher

Name: _____

Position: _____

Datum: _____

Unterschrift: _____

Auftragsverarbeiter

Name: _____

Position: _____

Datum: _____

Unterschrift: _____

Anlage 1

Datensicherheitskonzept

Maßnahmen zur Datenschutzkontrolle gemäß Art. 32 DS-GVO

Stand 08.08.2023

Bei Fragen zum XQueue Datenschutz und Informationssicherheit wenden Sie sich bitte an

heyData GmbH
Schützenstr. 5
10117 Berlin
support@heydata.eu

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 2

Aktuelle Unterauftragsverarbeiter

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