Vereinbarung
zum Datenschutz und zur Datensicherheit
in Auftragsverhältnissen nach § 11 BDSG

zwischen

.....

.....

.....
- Auftraggeber -

und

yQ-it GmbH
Aschaffenburger Str. 94 D
63500 Seligenstadt
- Auftragnehmer -

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in der Leistungsvereinbarung in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben.

§1 Gegenstand und Dauer des Auftrags

1. Der Auftragnehmer speichert und verarbeitet im Rahmen des vorliegenden Vertrages die durch den Auftraggeber erhobenen Daten.

2. Die Dauer des Auftrags richtet sich nach der Dauer des mit dem Auftraggeber geschlossenen Vertrages. Der Vertrag über einen Testzugang hat eine Laufzeit von 30 Tagen. Die Dauer des Vertrages über einen entgeltlichen Zugang wird durch den Auftraggeber beim Abschluss des Abonnements selbst ausgewählt. Dieser verlängert sich selbsttätig, wenn er nicht zuvor entsprechend der vereinbarten Kündigungsfrist gekündigt wird.

§2 Konkretisierung des Auftragsinhalts

1. Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten gemäß der in der Leistungsbeschreibung beschriebenen Funktionen der Software. Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

2. Der Auftragnehmer übernimmt den technischen Betrieb der Software. Die Erhebung und Nutzung der Daten sowie die Verarbeitung auf fachlicher Ebene erfolgt ausschließlich durch den Auftraggeber. Somit wird der Kreis der Betroffenen durch den Auftraggeber selbst bestimmt.

3. Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung zu einem Standort ausserhalb der Bundesrepublik Deutschland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

§3 Pflichten und Weisungsbefugnis des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung / - erhebung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

2. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

4. Die Berichtigung von personenbezogenen Daten erfolgt nur durch den Auftraggeber.

5. Der Auftragnehmer wird nur nach Weisung des Auftraggebers die personenbezogenen Daten, die im Auftrag verarbeitet werden, löschen oder sperren und dies nur soweit, wie dies dem Auftraggeber nicht selbst möglich ist.

6. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

7. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

§4 Pflichten des Auftragnehmers

1. Ergänzend zu den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer gemäß § 11 Abs. 4 BDSG die nachfolgenden gesetzlichen Pflichten.

2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Personen, mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis entsprechend § 5 BDSG verpflichtet. Dies umfasst auch die Belehrung über die in diesem Auftragsdatenverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

3. Der Auftragnehmer verpflichtet sich, die Ihm zur Verarbeitung überlassenen Daten ausschließlich im Rahmen der vertraglich festgelegten Weisungen zu verarbeiten. Der Auftragnehmer ist insbesondere nicht berechtigt, Daten an Dritte weiterzugeben.

4. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

5. Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technisch-organisatorischen Maßnahmen entsprechen § 9 BDSG und Anlage.

6. Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG informieren. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.

7. Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die Voraussetzungen für eine Bestellung nicht vorliegen.

§ 6 Technisch-organisatorische Maßnahmen

1. Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG. Der Anhang ist Bestandteil dieser Vereinbarung.

2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

§ 7 Kontrollrechte des Auftraggebers

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 soweit diese nicht Geschäftsgeheimnisse des Auftragnehmers berühren.
Das mit der Datenspeicherung beauftragte Rechenzentrum wird hinsichtlich der Einhaltung der Datenschutzvorschriften regelmäßig zertifiziert.

§ 8 Mitteilung bei Verstößen durch den Auftragnehmer

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

§ 9 Löschung von Daten und Rückgabe von Daten

Der Auftraggeber kann mithilfe der in der Software vorgesehenen Löschfunktionen jederzeit seine Daten selber löschen. Die Möglichkeiten der Datenrückgabe sind in der Onlinehilfe unter dem Stichwort “Export” einzusehen. Nach Beendigung des Saas-Vertrages löscht der Auftragnehmer die Daten entsprechend der Bedingungen des Saas-Vertrages oder auf schriftliche Anweisung des Kunden. Für die Einhaltung gesetzlicher Aufbewahrungsfristen ist der Auftraggeber selbst verantwortlich.

§ 10 Unterauftragsverhältnisse

Der Auftragnehmer ist berechtigt, zur Erfüllung des Vertrags Unterauftragsverhältnisse einzugehen, insbesondere mit Rechenzentrumsbetreibern. 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 Kontrollmaßnahmen zu ergreifen.

Auftraggeber:	Auftragnehmer:
.....	.....
Name, Vorname, Funktion	Name, Vorname, Funktion
.....	.....
Ort, Datum	Ort, Datum
.....	.....
Unterschrift	Unterschrift

Anhang:
Technisch-organisatorische Maßnahmen

Als Auftragsdatenverarbeiter verarbeitet der Auftragnehmer Daten im Auftrag seiner Auftraggeber. Ein Verlust oder unbefugtes Lesen oder Ändern dieser Daten hätte sowohl für die Auftraggeber als auch für den Auftraggeber selbst weitreichende und negative Konsequenzen. Der Auftragnehmer ist sich über die besondere Verantwortung für die Daten ihrer Kunden bewusst. Um dieser Verantwortung gerecht zu werden, hat der Auftragnehmer die erforderlichen technischen und organisatorischen Maßnahmen getroffen, diese Daten nach dem aktuellen Stand der Technik zu schützen.

Jeder Auftraggeber von Auftragsdatenverarbeitungen ist laut §11 BDSG dazu verpflichtet, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes zu überzeugen. Grundlage hierfür bildet diese Dokumentation. In der Anlage zu §9 Satz 1 BDSG sind die erforderlichen Maßnahmen konkretisiert. Um dem Auftraggeber eine Prüfung gemäß §11 BDSG zu erleichtern, richtet sich die Gliederung dieser Dokumentation nach der Anlage zu §9 Satz 1 BDSG.

1. Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Der Zutritt zum Rechenzentrum ist nur ausgewiesenen Mitarbeitern möglich und wird exakt erfasst. Die externen Rechenzentren genügen höchsten Ansprüchen und sind zertifiziert.

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, können nicht von Unbefugten genutzt werden. Es wird gewährleistet, dass nur autorisierte Mitarbeiter Zugang zu den verarbeiteten Daten haben. Hierfür werden folgende Sicherungsmaßnahmen verwendet:
- Eindeutige Identifizierung des Nutzers gegenüber dem System
- Festgelegte Berechtigungsstrukturen
- Verschlüsselung mittels SSL

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen zur Sicherstellung der Zugriffskontrolle:
- Restriktive differenzierte Rechtevergabe

- Die Remote Zugänge sind verschlüsselt und so gering wie möglich gehalten in der Anzahl.
- Es existieren Testsysteme.
- Die zentralen Systeme sind in einem dedizierten Raum verschlossen.

4. Weitergabekontrolle

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.

Es wird gewährleistet, dass Daten ausschliesslich über verschlüsselte Verbindungen zwischen dem Server und des Client des Kunden außerhalb des Rechenzentrums übertragen werden. Hierbei kommt das SSL verschlüsselte HTTP Protokoll (HTTPS) zum Einsatz.

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Die Eingabekontrolle wird gewährleistet indem Protokolleinträge zu jeder Änderung von Daten erstellt werden. Diese sind Teil der Kundendatenbank und sind vom betroffenen Kunden direkt über die Software einsehbar. Die Protokolleinträge sind nicht änderbar oder löschbar.

6. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Ein mehrstufiges Sicherheitskonzept stellt die Verfügbarkeit der Daten sicher. Zum einen sind alle physikalischen Datenträger (Festplatten) als RAID-Verbund ausfallsicher angelegt. Der Status der Datenträger wird laufend automatisch überwacht und defekte Festplatten sofort ausgetauscht.

Ausserdem werden die Kundendaten jede Nacht gesichert und verschlüsselt in einem anderen Brandabschnitt im Rechenzentrum gespeichert und nach 7 Tagen überschrieben.

7. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Jeder Kunde hat eine eigene logische Datenbank mit einem eigenen Benutzerkonto innerhalb eines Datenbankmanagementsystems (DBMS), welches mehrere dieser logischen Datenbanken verwaltet.
Der Applikationsserver, der die fachliche Programmlogik ausführt, öffnet zum Schreiben oder Lesen der personenbezogenen Daten nur Verbindungen auf die Datenbank des jeweiligen Kunden.