Vertrag über Auftragsverarbeitung

der SQL Projekt AG, Franklinstr. 25a, 01069 Dresden

Zwischen

Firma: _____

Straße, Nr.: _____

PLZ, Ort: _____

- Auftraggeber -

und

SQL Projekt AG
Vertreten durch den Vorstand
Herrn Jens Gärtner
Herrn Stefan Ehrlich
Franklinstraße 25 a
01069 Dresden

- Auftragnehmer -

wird folgender Vertrag geschlossen:

§ 1 Vertragsgegenstand und Verantwortlichkeit

1.
Mit separatem Auftrag, Vertragsnummer: _____ (nachfolgend als Leistungsvereinbarung bezeichnet) hat der Auftraggeber den Auftragnehmer mit der befristeten Überlassung der Software SALIA® (nachfolgend bezeichnet als Software) und des SALIA® Kundenportals Basis 10 beauftragt.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten im Auftrag des Auftraggebers i.S.v. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

2.
Die Verarbeitung durch den Auftragnehmer umfasst Tätigkeiten, die in diesem Vertrag und in der Leistungsvereinbarung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich. Der Auftraggeber ist Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO.

3.
Die Weisungen werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4.
Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

§ 2 Weisungsbefugnis des Auftraggebers

1.
Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

2.
Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

3.
Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. 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.

4.
Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

5.
Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen,

bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

§ 3 Leistungen des Auftragnehmers

1. Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Der Auftragnehmer erbringt im Auftrag des Auftraggebers folgende Leistungen:

- Implementierung der Software SALIA® in die IT-Umgebung des Auftraggebers und Konfiguration
- Implementierung von Updates
- Wartungs- und Pflegearbeiten bzgl. der Software, insbesondere mittels Fernwartung
- Aufbewahren des Kundenportal-Servers des Auftraggebers
- Bereitstellung der Software für den Kundenportal-Server des Auftraggebers.

2. Art der Daten

Folgende Datenarten /-kategorien sind Gegenstand der Erhebung, Verarbeitung und Nutzung personenbezogener Daten:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Vertragsabrechnungsdaten
- Kundenhistorie
- Planungs- und Steuerungsdaten
- kundenbezogene Dokumente

3. Kreis der Betroffenen

Der Kreis der durch den Umgang mit den personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst folgende Personenkategorien:

- Kunden
- Mitarbeiter
- Geschäftspartner

4. Gebiet

Die Erhebung, Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

5. Technisch-organisatorische Maßnahmen

a.
Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO sowie die Maßnahmen gemäß **Anlage 1**.

b.
Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Im Falle der Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

c.
Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots (vgl. **Anlage 1**), sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand.

d.
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 des Auftraggebers eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Verfügung zu stellen.

6. Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren.

7. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

a) Benennung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten i.S.v. Art. 37 DSGVO. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Die Kontaktdaten des zum Zeitpunkt des Abschlusses dieses Vertrages beim Auftragnehmer bestellten Datenschutzbeauftragten sind in der Anlage 2 aufgeführt. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

b) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Ziffer 7 a) kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich

nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

c) Die Wahrung des Datengeheimnisses entsprechend Art. 28 Abs. 3 S. 2 b) DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

d) Die unverzügliche Information des Auftraggebers, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

e) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

8. Fernwartung

1.
Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

2.
Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

3.
Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

9. Unterauftragsverhältnisse

a) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der **Anlage 3** aufgeführten Unternehmen als Subunternehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Der Auftraggeber erklärt sich mit dem Tätigwerden dieser Subunternehmer einverstanden.

b) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftraggeber hat die Möglichkeit, gegen die Begründung weiterer Unterauftragsverhältnisse Einspruch zu erheben.

c) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

d) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragte zu benennen.

e) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

f) Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).

g) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

h) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse gemäß § 4 dieses Vertrages des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

g) 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 gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

h) Die Wartung und Pflege von IT-Systemen oder Applikationen stellen zustimmungspflichtige Unterauftragsverhältnisse und Auftragsverarbeitung i.S.v. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

§ 4 Kontrollrechte des Auftraggebers

1.
Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

2.
Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.v. § 3 Ziffer 1 erforderlich ist.

3.
Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen. Der Auftraggeber kann sich darüber hinaus vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

4.
Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle i.S.v. § 3 Ziffer 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

5.
Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß **Anlage 1** nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B.

Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

6.
Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber 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 Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

7.
Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.v. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

§ 5 Pflichten des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 6 Pflichten des Auftragnehmers

1.
Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen daten-schutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn, mit der Verarbeitung beschäftigte Personen oder durch Dritte erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

2.
Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

3.
Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

4.
Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

5.
Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen.

6.
Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis Art. 36 DS-GVO genannten Pflichten.

§ 7 Anfragen und Rechte Betroffener

1.
Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

2.
Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

3.
Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

4.
Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

§ 8 Löschung von Daten und Rückgabe von Datenträgern

1.
Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber

auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung ist in geeigneter Weise zu dokumentieren und diese Dokumentation auf Anforderung vorzulegen.

2.
Der Auftragnehmer ist berechtigt, Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 9 Auftragsdauer, Kündigung

1.
Die Dauer dieses Auftrags entspricht der Dauer der Leistungsvereinbarung, sofern sich aus den Besonderheiten des vorliegenden Auftrags nichts anderes ergibt.

2.
Das Recht zur außerordentlichen fristlosen Kündigung wegen Vorliegen eines wichtigen Grundes bleibt für jede Vertragspartei unberührt.

§ 10 Anlagen

Sämtliche, in diesem Vertrag in Bezug genommenen Anlagen sind Bestandteil dieses Vertrages.

Es handelt sich hierbei um folgende Anlagen:

- Anlage 1 Technische und organisatorische Maßnahmen
- Anlage 2 Datenschutzbeauftragter des Auftragnehmers
- Anlage 3 Unterauftragsverhältnisse.

§ 11 anwendbares Recht, Erfüllungsort, Gerichtsstand

1.
Auf vorliegenden Vertrag findet deutsches Recht Anwendung.

2.
Erfüllungsort ist der Sitz des Auftragnehmers, d.h. Dresden.

3.
Für Streitigkeiten aus diesem Vertrag ist ausschließlicher Gerichtsstand Dresden.

§ 12 Schriftformklausel

Nebenabreden sind nicht getroffen. Änderungen oder Ergänzungen dieses Vertrages bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

Dies gilt auch für den Verzicht auf dieses Formerfordernis.

§ 13 Salvatorische Klausel

Sollten eine oder mehrere Bestimmungen dieses Vertrages unwirksam sein oder werden, so wird dadurch die Wirksamkeit des Vertrages im Übrigen nicht berührt. Vielmehr wird die unwirksame Bestimmung durch eine wirksame Regelung ersetzt, die in ihrer Auswirkung der unwirksamen Bestimmung nahekommt. Entsprechendes gilt im Fall einer Vertragslücke.

_____	Dresden,_____
Ort, Datum	Ort, Datum
_____	_____
(Auftraggeber)	(Auftragnehmer – SQL Projekt AG)

Anlage 1 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen gewährleistet durch:
  - Zugang durch Haupteingang und Tiefgarage nur mit Schlüssel möglich,
  - Sicherung der einzelnen Büroetagen durch eine gemeinsame Alarmanlage außerhalb der Bürozeiten (Schlüssel und Key für die Alarmanlage hat jeder Mitarbeiter),
  - Besucher müssen sich über eine Gegensprechanlage identifizieren und werden durch den Besuchten in Empfang genommen
  - Zutritt zu den Serverräumen hat nur der Administrator und der Vorstand
  - Dokumentation der Vergabe und Rückgabe von Schließmitteln
- Zugangskontrolle
  Keine unbefugte Systembenutzung, gewährleistet durch:
  - Mitarbeiter müssen sich gegenüber dem Active Directory identifizieren und erhalten dadurch im internen Netz ihre Berechtigungen auf Basis eines Rollenkonzepts.
  - Passwörter müssen regelmäßig geändert werden und aus unterschiedlichen Zeichenmengen (Groß- und Kleinschreibung, Sonderzeichen, Zahlen gemäß Passwortrichtline) bestehen.
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, gewährleistet durch:
  - Benutzerrechte der Mitarbeiter werden über ein Rollenkonzept vergeben
  - Onlinezugriffe sind grundsätzlich mit dem Auftraggeber abzusprechen. Der Zugriffssicherungscode wird vom Auftragnehmer an den Auftraggeber telefonisch übermittelt. Der Auftraggeber muss dem Zugriff des Auftragnehmers prinzipiell erst zustimmen, bevor der Zugriff auf das System des Auftraggebers erfolgen kann.
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, erfolgt durch:
  - Im Rahmen des Auftrages werden im Normalfall keine Daten des Auftraggebers beim Auftragnehmer gespeichert. Sollten durch Weisung des Auftraggebers Daten beim Auftragnehmer zu Testzwecken gespeichert werden, so werden diese von Daten anderer Auftraggeber sowie anderer Test- und Produktionsdaten getrennt.

2. Integrität

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich, durch:
  - Sollte eine Übertragung von Dateien notwendig sein, so erfolgt diese über Remotedesktop bzw. vor Ort beim Auftraggeber. Die verschlüsselte Übertragung hängt von der Konfiguration des Auftraggebers ab.
  - Eine Verwendung von Datenträgern zur Übermittlung personenbezogener Daten ist derzeit nicht vorgesehen.
  - Unaufgefordert zugesandte E-Mails mit Dateianhängen werden ungesehen gelöscht.

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
    - Onlinezugriffe werden protokolliert im Normalfall durch pcvisit SupportJournal

3. Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, durch:
    - Einhaltung der Brandschutzvorschriften
    - Benennung eines Brandschutzhelfers
    - Klimaanlage im Serverraum
    - Feuerlöscher auf jeder Etage
    - Überspannungsschutz
    - System-Monitoring
    - Datensicherheitsplan
    - Wiederanlaufplan
    - Raid-Controller
    - Mitarbeiterverpflichtung auf Datengeheimnis

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutzleitlinie
- Datensicherheitsplan
- Wiederanlaufplan
- Verfahrensverzeichnis
- Interne Richtlinien und Arbeitsanweisungen
- ISO 9001 Zertifizierung, regelmäßige Auditierung durch Externe
- Regelmäßige Sensibilisierungs-/Schulungsmaßnahmen zur Informationssicherheit und zum Datenschutz
- Datenschutzfreundliche Voreinstellungen
- Auftragskontrolle
    - keine Auftragsverarbeitung im Sinne ohne entsprechende schriftliche Weisung des Auftraggebers

Anlage 2 - Datenschutzbeauftragter

Die Benennung eines Datenschutzbeauftragten bestimmt sich nach der DSGVO und dem BDSG (neu).

Als Datenschutzbeauftragter wurde benannt:

Dresdner Institut für Datenschutz
Hospitalstraße 4
01097 Dresden

Unser Datenschutzteam erreichen Sie über die E-Mail:
datenschutz@sql-ag.de

Für vertrauliche Anfragen an den Datenschutzbeauftragten kontaktieren Sie bitte:
zentrale@dids.de

Anlage 3 – Subunternehmer

1) Mit der Durchführung folgender Arbeiten:
   - Aufbewahren des Kundenportal-Servers des Auftraggebers

   hat die SQL Projekt AG einen Subunternehmer beauftragt.

   Es handelt sich dabei um die Firma:

   Host Europe GmbH
   Welserstr. 14
   51149 Köln

2) Mit der Durchführung folgender Arbeiten:
   - Bereitstellung der Fernwartungssoftware

   hat die SQL Projekt AG einen Subunternehmer beauftragt.

   Es handelt sich dabei um die Firma:

   pcvisit Software AG
   Manfred-von-Ardenne-Ring 20
   01099 Dresden