Vertrag
über die Verarbeitung personenbezogener Daten
(Auftragsverarbeitung gemäß Art. 28, 29 DSGVO)

zwischen dem Unternehmen
(wie im Handelsregister eingetragen)

Firmenname .....

Strasse .....

Ort .....

- nachstehend Auftraggeber genannt -

und dem Unternehmen
(wie im Handelsregister eingetragen)

IQUINOX AG
Curiestraße 2
70563 Stuttgart

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

Präambel

Dieser Datenschutzvertrag regelt den Schutz personenbezogener Daten bei der Datenverarbeitung im Auftrag. Lässt eine verantwortliche Stelle (Auftraggeber) die Verarbeitung von personenbezogenen Daten durch eine andere Stelle (Auftragnehmer) ausführen, ist gemäß Art. 28 DSGVO ein schriftlicher Vertrag

zur Auftragsverarbeitung abzuschließen. Sofern in diesem Vertrag der Begriff Datenverarbeitung oder Verarbeitung von Daten verwendet wird, wird die Definition der Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO gemeint: zur Datenverarbeitung zählt neben dem Speichern, Verändern, Übermitteln, Sperren und Löschen auch das Bereithalten von Daten zur Einsicht oder zum Abruf durch einen Dritten.

Die Verantwortung für die datenschutzkonforme Verarbeitung der personenbezogenen Daten verbleibt beim Auftraggeber. Nach Art. 29 DSGVO darf der Auftragnehmer die Daten nur auf Weisung des Auftraggebers verarbeiten. Verstößt der Auftragnehmer dagegen, indem er z.B. Zwecke der Verarbeitung selbst bestimmt, wird er nach Abs. 28 Abs. 10 gegenüber Betroffenen selbst zum Verantwortlichen.

Aus diesem Grund regeln Auftraggeber und Auftragnehmer Nachfolgendes:

Dieser Vertrag konkretisiert die gesetzlichen Rechte und Pflichten, die sich für die Vertragsparteien aus dem anwendbaren Datenschutzrecht und insbesondere aus dem Bundesdatenschutzgesetz, ab dem 25.05.2018 aus der Datenschutzgrundverordnung, nachfolgend auch „DSGVO“ sowie der nationalen Datenschutzgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet (Anlage 1). Er findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag / Hauptverträgen (in Anlage 1 aufgeführt) in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Als solche Tätigkeiten kommen insbesondere ein Remotezugriff auf das IT-System des Auftraggebers via TeamViewer, der Umgang mit einer Echtdaten enthaltenden Backup-Datei, vor allem im Zusammenhang mit Supportanfragen, in Betracht, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf mit dem Laufzeitende des letzten verbleibenden, in Anlage 1 aufgeführten Hauptvertrages.

Der Auftragnehmer erbringt diverse Dienstleistungen im Umfeld der Softwarelösungen aus dem Hause der Sage GmbH, beispielsweise im Bereich der Softwareimplementierung, Softwareschulungen, Datenbankpflege, Softwarebetreuung; auch per Fernwartung. Der Auftraggeber beauftragt den Auftragnehmer regelmäßig zur Erbringung dieser angeführten oder anderen artverwandten Leistungen zu den bekannten Dienstleistungshonoraren. Der Auftragnehmer verarbeitet dabei nicht immer, aber regelmäßig personenbezogene Daten für den Auftraggeber gemäß Artikel 28 DSGVO.

Verweigert der Auftraggeber die Unterzeichnung des Vertrags, so ist der Auftragnehmer kraft Gesetz nicht mehr in der Lage, seine Betreuung weiter zu garantieren. Die zwischen Auftraggeber und Auftragnehmer geschlossenen Hauptverträge gemäß Anlage 1 bleiben davon unberührt.

Begründet durch die Vielzahl der betreuten Kunden und um ein einheitliches Vertragswerk mit allen Kunden zu garantieren, übersendet der Auftragnehmer dem Auftraggeber seinen Vertrag. Zur Sicherstellung datenschutzrechtlicher Bestimmungen, zur lückenlosen Nachverfolgbarkeit der Dokumente sowie zur Gewährleistung der rechtmäßigen Authentifizierung des Unterzeichnenden übersendet der Auftragnehmer seinen Datenschutzvertrag vorwiegend mittels DocuSign; eine Software des globalen Marktführers für elektronische Signaturen. Nähere Informationen dazu erhält der Auftraggeber auf der Internetseite des Auftragnehmers (www.iquinox.de) oder des Anbieters (www.docusign.de).

Anmerkung: Auch wenn Artikel 28 DSGVO inhaltlich vieles aus dem alten Recht laut § 11 BDSG aufgreift, gibt es eine wesentliche Neuerung bzw. wichtige Erleichterung: laut BDSG waren die Verträge noch schriftlich abzuschließen, was bedeutete, dass die Unterschriften der Vertragsparteien erforderlich waren. Jetzt

ist es aber möglich, Verträge zur Auftragsdatenverarbeitung auch in einem elektronischen Format abzuschließen. Diesbezüglich ist der Gesetzestext eindeutig; dem europäischen Gesetzgeber genügt es, die nach der DSGVO geforderte Transparenz- und Rechenschaftspflicht durch elektronische Signaturen zu erfüllen. Eine händische Unterschrift ist somit nicht mehr erforderlich.

Stand heute lässt sich rechtlich nicht zweifelsfrei sagen, ob geschlossene AV-Verträge lediglich per Mail oder per nicht geschützten Dokumenten überhaupt einen wirksamen AV-Vertrag begründen. Aus den zuvor genannten Gründen übersendet der Auftragnehmer seine Verträge daher vorsorglich per elektronischer Signatur des Anbieters DocuSign mit Zugriffsauthentifizierung.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Verarbeitung: Verarbeitung umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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.

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete dokumentierte Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in dokumentierter Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Hauptverträge, welche zwischen Auftraggeber und Auftragnehmer unter Bezugnahme auf die Allgemeinen Geschäfts- und Supportbedingungen des Auftragnehmers vor dem 25. Mai 2018 geschlossen wurden, enthalten nur die Datenschutzanweisungen, welche laut geltendem Recht vor dem 25. Mai 2018 Gültigkeit hatten.

§ 2 Gegenstand des Auftrags, Anwendungsbereich

(1) Der Auftragnehmer prüft und wartet automatisierte Verfahren oder Datenverarbeitungsanlagen im Auftrag, insbesondere die von ihm im Rahmen eines getrennten Vertragsverhältnisses überlassene Standardsoftware und bietet im Rahmen seiner Supportangebote weitergehende Hilfestellungen im Umgang mit der Software an. Hierzu bedient sich der Auftragnehmer nach Absprache mit dem Mitarbeiter des Auftraggebers auch der Fernwartung mittels TeamViewer oder anderen Systemen. Ferner bietet er Softwarelösungen auch im Rahmen von Hosting, ASP, SaaS oder Cloud basierender Angebote an. Im Rahmen dieser Tätigkeiten kann in besonderen Konstellationen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die umfassten Tätigkeiten sind in der Leistungsbeschreibung des Hauptvertrages, den Allgemeinen Geschäfts- und Supportbedingungen des Auftragnehmers und/oder der Leistungsbeschreibung der Sage Wartungsverträge konkretisiert. Die Hauptverträge sind ferner in Anhang 1 zu dieser Vereinbarung, unter Nennung der jeweils betroffenen Datenkategorien, aufgeführt. Die Auflistung wird von den Parteien bei Wegfall oder Neuabschluss eines weiteren Hauptvertrages, der auch Auftragsverarbeitung zum Gegenstand hat, fortlaufend aktualisiert.

(2) Die nach diesem Vertrag den Parteien auferlegten Rechte und Pflichten gelten nur während der Laufzeit des Vertrages und innerhalb dieses Zeitraums nur in den Zeitabschnitten bei denen tatsächlich eine Auftragsverarbeitung durchgeführt wird oder eine vergleichbare Gefahrenlage für personenbezogene Daten, für die der Auftraggeber verantwortliche Stelle ist, gegeben ist.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Darüber hinaus kann sich im Einzelfall für den Auftragnehmer eine gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten ergeben.

In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die betreffende rechtliche Verpflichtung verbietet eine solche Mitteilung wegen wichtigen öffentlichen Interesses.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des anwendbaren Datenschutzrechts gerecht wird. Er wird die geeigneten und gesetzlich erforderlichen technischen und organisatorischen Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet insbesondere

- die Verschlüsselung personenbezogener Daten;

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen (TOMs) wird als Anlage 2 diesem Vertrag beigefügt.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

(4) Der Auftragnehmer ist aufgrund gesetzlicher Bestimmungen zurzeit nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet, da regelmäßig weniger als zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind; hierbei sind Vollzeit- und Teilzeitkräfte ebenso wie Aushilfen berücksichtigt. Der Auftragnehmer ist aufgrund gesetzlicher Bestimmungen ebenfalls nicht verpflichtet, einen externen Datenschutzbeauftragten zu bestellen. Tut er dies auf freiwilliger Basis trotzdem, teilt er dem Auftraggeber die Kontaktdaten des bestellten externen Datenschutzbeauftragten mit.

(5) Im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen unterstützt der Auftragnehmer den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der gesetzlichen Pflichten, die den Auftraggeber als Verantwortlichen treffen (u.a. bei der Wahrnehmung von Betroffenenrechten, der Durchführung von Kontrollen durch die zuständige Datenschutzaufsichtsbehörde sowie bei der Erfüllung gesetzlicher

Informationspflichten gegenüber Betroffenen und Datenschutzbehörden). Der Auftraggeber erstattet dem Auftragnehmer durch die Unterstützung entstehende Kosten und den Arbeitsaufwand. Können sich die Parteien nicht über den Umfang der Erstattung einigen, werden die Kosten, die der Auftragnehmer für erforderlich halten durfte, vom Auftraggeber in vollem Umfang erstattet.

(6) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und auf Verlangen in geeigneter Weise gegen Gebühr nachzuweisen.

(8) Die Auftragsverarbeitung darf nur innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Eine Verlagerung in ein Drittland außerhalb dieses Gebietes bedarf der vorherigen Zustimmung des Auftraggebers.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne des anwendbaren Datenschutzrechts für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer verantwortlich. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber.

(2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen (Einzelweisung). Der Auftraggeber trägt hierdurch anfallende

Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.

(3) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund von angeblich unrechtmäßigen Datenverarbeitungen Ansprüche geltend machen, wird der Auftraggeber, soweit diese angeblich unrechtmäßigen Verarbeitungen auf Vorsatz oder Fahrlässigkeit des Auftraggebers beruhen, den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt, erstattet der Auftraggeber dem Auftragnehmer die Kosten.

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 5 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Die hierfür erforderlichen Informationen werden dem Auftraggeber gemäß nachfolgendem Absatz zur Verfügung gestellt.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag geregelten Pflichten zur Verfügung. Er ermöglicht und trägt bei zu Überprüfungen, einschließlich Inspektionen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

(3) Die Häufigkeit der Kontrollen soll maximal alle 18 Monate erfolgen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen. Die dem Auftragnehmer durch die Kontrollen entstehenden Kosten sind vom Auftraggeber zu erstatten.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt durch eine Vor-Ort Kontrolle durch die Vorlage eines geeigneten Testats des, soweit vorhanden, betrieblichen Datenschutzbeauftragten, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. externer Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor) oder einer geeigneten Datenschutz-Zertifizierung durch eine zugelassene Stelle erbracht werden ("Zertifizierungsurkunde"). Die Zertifizierungsurkunde muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß beiliegender Anlage 2 zu überzeugen.

§ 6 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen bei Notwendigkeit die in der Anlage 3 benannten weiteren Auftragsverarbeiter (Subunternehmer) einschaltet. Über eine Änderung der in der Anlage 3 genannten Subunternehmer wird der Auftragnehmer den Auftraggeber informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Im Übrigen ist die Beauftragung von Subunternehmern durch den Auftragnehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nur aus wichtigem, dem Auftragnehmer nachzuweisendem Grund verweigert werden. Im Fall der Einschaltung von im Sinne der §§ 15 ff.

AktG mit dem Auftragnehmer verbundenen Unternehmen als Subunternehmer erteilt der Auftraggeber hiermit schon jetzt ausdrücklich seine Zustimmung.

(3) Der Auftragnehmer wird weiteren Auftragsverarbeitern vertraglich dieselben Pflichten wie nach diesem Vertrag auferlegen, einschließlich hinreichender Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls gegen Gebühr auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen.

§ 7 Informationspflichten

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des anwendbaren Datenschutzrechts liegen.

§ 8 Informationsrechte

Der Auftraggeber erklärt sich damit einverstanden, dass ihn der Auftragnehmer mit Produkten und Dienstleistungen, welche sich aus den Hauptverträgen ergeben, insbesondere mit Softwareprodukten der Sage Software GmbH und entsprechenden Dienstleistungen via Post und/oder Mail bewirbt.

Der Auftraggeber erklärt sich ebenfalls damit einverstanden, dass ihm der Auftragnehmer Angebote, Auftragsbestätigungen, Lieferscheine und/oder Rechnungen auch weiterhin per Post, Telefax oder Mail ohne spezielle Datenverschlüsselungen übersenden darf, sofern darin außer des Firmennamen, der Anschrift, der Mailadresse und des Ansprechpartners keine weiteren personenbezogenen datenschutzwürdigen Informationen stehen.

§ 9 Vertragsdauer und -beendigung

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des bestehenden Hauptvertrages.

(2) Nach Abschluss der Erbringung der Verarbeitungstätigkeiten bzw. nach Beendigung der Vereinbarung hat der Auftragnehmer nach Aufforderung des Auftraggebers all diejenigen personenbezogenen Daten zu löschen, die gemäß aktueller Rechtsprechung als schützenswert eingestuft sind. Dies gilt nicht, soweit für den Auftragnehmer auf Grundlage des anwendbaren Datenschutzrechts eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z.B. gesetzliche Aufbewahrungspflicht).

(3) Der Auftraggeber legt die Maßnahmen zur Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Dadurch resultierende zusätzliche Kosten durch die Herausgabe oder Löschung der Daten sind vom Auftraggeber zu tragen.

§ 10 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DSGVO und/oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung 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.

(3) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Ausschließlicher Gerichtsstand ist Stuttgart.

(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Weisungsbefugnisse

Der Unterzeichner seitens des Auftraggebers bestätigt, dass die nachgenannten Personen von ihm schriftlich zu Weisungsbefugten bestellt worden sind.

Unterschriftsberechtigt für Auftraggeber: _____

Weisungsbefugt für den Auftraggeber ist: _____

Weisungsbefugt für den Auftraggeber ist: _____

Weisungsempfänger beim Auftragnehmer: Jens Nickelsen, Vorstand

_____ Stuttgart, den 22. Mai 2018

Ort und Datum

_____ _____

Auftraggeber

Auftragnehmer
IQUINOX AG, Stuttgart
Jens Nickelsen, Vorstand

Bitte beachten Sie, dass diejenige Person, die diese Vereinbarung als Auftraggeber unterzeichnet, auch zur Unterschrift berechtigt ist.

Anlage 1

Art und Kategorien der Datenverarbeitung

Folgende Hauptverträge liegen der Datenverarbeitung zugrunde:

- ☑ Hauptvertrag Sage Software-Wartungsvertrag bei gekaufter Software
- ☑ Hauptvertrag Sage Software-Nutzungsvertrag bei gemieteter Software
- ☑ Sage Software Anwenderunterstützung ohne vertragliche Vereinbarung
- ☑ Programmierungen für alle unten angeführten Sage Softwarelösungen

Es ist möglich, dass der Auftraggeber mehrere Hauptverträge gleichzeitig hat

Folgende Datenarten sind Gegenstand dieses Auftrags. Zutreffendes ist vom Auftraggeber anzukreuzen:

		Kategorien *	Subunternehmer
☐	Globales Einverständnis für alle aktuellen und künftigen Softwareprodukte aus dem Hause der Sage Software GmbH (Frankfurt) und für Softwareprodukte, die zur Verwendung der Sage Softwareprodukte notwendig sind.	1 bis 8	1, Sage, Frankfurt

Oder für die nachfolgenden Sage Einzel-Softwarelösungen:

☐	Sage Kundenkontaktmanagement CRM	1, 3, 8	1, Sage, Frankfurt
☐	Sage New Classic Finanzbuchhaltung Sage New Classic, Classic Line, Standard oder Professionell	1 bis 6	1, Sage, Frankfurt
☐	Sage New Classic Auftragsbearbeitung Sage New Classic, Classic Line, Standard oder Professionell	1 bis 5	1, Sage, Frankfurt
☐	Sage New Classic Produktion Sage New Classic, Classic Line, Standard oder Professionell	2, 3, 7	1, Sage, Frankfurt
☐	Sage 100 Rechnungswesen Sage 100, Sage 100 Cloud, Office Line. Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1 bis 6	1, Sage, Frankfurt

		Kategorien*	Subunternehmer
☐	Sage 100 Warenwirtschaft Sage 100, Sage 100 Cloud, Office Line. Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1 bis 5	1, Sage, Frankfurt
☐	Sage 100 Produktion PPS Sage 100, Sage 100 Cloud, Office Line. Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	2, 3, 7	1, Sage, Frankfurt
☐	Sage Aufgabencenter Sage New Classic oder Classic Line; Standard, Professional; Sage 100, Sage 100Cloud, Office Line, Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1, 2, 4 bis 7	1, Sage, Frankfurt
☐	Sage Dokumentenmanagement DMS Sage New Classic oder Classic Line; Standard, Professional; Sage 100, Sage 100Cloud, Office Line, Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1 bis 6	1, Sage, Frankfurt
☐	Sage E-Bilanz Sage New Classic oder Classic Line; Standard, Professional; Sage 100, Sage 100Cloud, Office Line, Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1, 2, 4 bis 6	1, Sage, Frankfurt
☐	Sage Webclient Sage New Classic oder Classic Line; Standard, Professional; Sage 100, Sage 100Cloud, Office Line, Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1 bis 7	1, Sage, Frankfurt
☐	Sage XRM Sage 100, Sage 100 Cloud, Office Line. Office Line Evolution; Basic oder Business, Flex oder Complete; Office Line 24	1, 2, 3, 8	1, Sage, Frankfurt
☐	Sage HR Personalabrechnung inklusive aller Sage HR Zusatzmodule	Siehe unten *	1, Sage, Frankfurt

(*) Betroffene Datenkategorien: Alle personen- und unternehmensbezogenen Daten, die zur Abrechnung der Mitarbeiter und zur Meldung an das Finanzamt, Krankenkassen und sonstigen Meldestellen benötigt werden. Beim Modul Bewerbermanagement alle Daten, die ein Bewerber zu Bewerbungszwecken eingeben muss; dies umfasst ggf. auch Bilder und Kopien von Dokumenten. Bei der Digitalen Personalakte alle Firmenstammdaten, Personalstammdaten und Personalbewegungsdaten sowie bei Nutzung der elektronischen Personalakte Verträge, Belege, Auswertungen und sonstige Dokumente aus dem Personalbereich. Subunternehmer: Sage Software GmbH.

Datenkategorien *

1. Kontaktdaten und -historie bzgl. natürlicher Personen
2. Daten zur Geschäftshistorie
3. Daten von Mitarbeitern/Anwendern des Systems
4. Daten zu finanziellen Transaktionen
5. Daten zu Bankverbindungen und Zahlungsarten
6. Daten zur Vermögens- und Ertragssituation
7. Daten zu Arbeitszeiten und Abläufen
8. Sonstige personenbezogene Daten der Kontakte

Anlage 2

Technische und organisatorische Maßnahmen

(Datenschutzmanagement der IQUINOX AG)

Datensicherungsmaßnahmen betreffend Softwarepflegeleistungen

(Zugriffe im Rahmen der Fehleranalyse Software und Remote-Support)

Um die von ihm verarbeiteten personenbezogenen Daten zu schützen, hat der Auftragnehmer angemessene technische und organisatorische Sicherheitsmaßnahmen, einschließlich der folgenden Maßnahmen umgesetzt:

Vertraulichkeit gemäß Art. 32 Abs. 1 DSGVO

Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Der allgemeine Zutritt zum Gebäude erfolgt über ein zweifaches Zutrittskontrollsystem (Gebäude, Büro) via Codekarten. Das Gebäude ist täglich von 18 Uhr bis 8 Uhr am Folgetag sowie an Wochenenden und Feiertagen generell verschlossen. Die Vergabe der Codekarten wird dokumentiert. Alle Büroräume sind verschlossen und können nur von Mitarbeitern von Innen geöffnet werden. Besucher müssen sich am Empfang anmelden und dürfen nur in Begleitung die Räumlichkeiten betreten. Der Zutritt zu den Server-Racks wird über einen Zutrittskontrollsystem (Schlüssel) reguliert; Zugang haben nur ausgewählte Mitarbeiter der IT. Der Standort des Servers befindet sich in der Welzenwilerstraße in 72074 Tübingen, Deutschland. Der Standort für die redundante und verschlüsselte Datensicherung via Cloud befindet sich ebenfalls in Deutschland; Josef-Schüttler-Str. in 78224 Singen.

Zugangskontrolle

Maßnahmen, die geeignet sind, den Zugang Unbefugter zu verhindern.

Reduktion der zugriffsberechtigten Personen auf ein Minimum. Für die Anmeldung an das Netzwerk ist ein 8 stelliges Kennwort erforderlich. Dabei sind Zahlen und Sonderzeichen zu verwenden sowie Groß- und Kleinschreibung zu beachten. Alle Kennwörter werden nach 180 Tagen geändert und entsprechend protokolliert. Eine Aktivierung des Bildschirmschoners erfolgt automatisch nach 15 Minuten und kann nur über Passworteingabe wieder freigegeben werden.

Benutzerauthentifizierung wird mittels eines zentralen Verzeichnisdienstes abgebildet. Grundsätzlich und soweit nicht technisch notwendig, ist ein Zugang zu Auftragsdaten nur mittels personifizierten Accounts zugelassen. Das System wird durch eine Firewall ständig überwacht. Eine Antivirus-Software auf Systemebene und darüber hinaus für das Mail-System ist je Client installiert. Es werden ausschließlich IT-Systeme eingesetzt, die vom Hersteller durch regelmäßige Sicherheitsupdates unterstützt werden. W-LAN ist zwar grundsätzlich vorhanden, wird aber aktuell nicht eingesetzt.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten, ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert und entfernt werden können.

Das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern wird verhindert durch die Nutzung von Datenträgern nur auf Kundenwunsch, der Vernichtung von Datenträgern durch Verwendung von geeigneten Schreddern.

Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten wird gewährleistet durch die automatische Prüfung der Berechtigung durch ein Passwort, einer benutzerdefinierten Menüsteuerung je nach Berechtigung, die differenzierte Zugriffsberechtigung auf unterschiedliche Programme und eine Differenzierung der Verarbeitungsmöglichkeiten; Lesen, Ändern, Löschen.

Trennungsgebot

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

Die unterschiedliche und getrennte Verarbeitung wird gewährleistet durch softwareseitigen (organisatorischen) Ausschluss via Trennung der Mandanten, der Trennung zwischen Produktivumgebung und der Verwendung getrennter Test- bzw. Entwicklungsumgebungen sowie durch getrennte Datenbanken in Hyper-V-Aufteilungen; virtuelle Maschinen innerhalb des Systems.

Integrität gemäß Art. 32 Abs. 1 DSGVO

Kontrolle der Weitergabe

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder Ihres Transports zum Empfänger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch die Verwendung eines SFTP Server und eine SSL/HTTPS Verschlüsselung.

Bei Datenversendung per Mails verwenden wir als Auftragnehmer eine marktführende Datenschutzsoftware des Herstellers FTAPI mit der Möglichkeit, bei der Versendung je nach Datensensibilität unterschiedliche Sicherheitsstufen auszuwählen, bis hin zu echten Ende-zu-Ende-Verschlüsselungen.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft bzw. festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht wurden.

Alle Netzwerkanmeldungen und Netzwerkabmeldungen sowie sämtliche Transaktionen (z.B. Neuanlagen, Veränderungen, Löschungen) werden protokolliert. Die Protokolle werden nach 6 Monaten gelöscht. Die Protokolle werden hinsichtlich unberechtigter Zugriffe analysiert. Zur Löschung von Daten auf Papierform stehen Aktenvernichter zur Verfügung.

Der Auftragnehmer erhebt, verändert oder löscht personenbezogene Daten vorwiegend im Rahmen der eigenen Kundenkontaktsysteme, eine Verarbeitung für andere Zwecke erfolgt nicht bzw. nur auf ausdrücklichen Kundenwunsch.

Verwendet der Auftragnehmer eine Fernwartungssoftware, vorwiegend die des marktführenden Herstellers TeamViewer, so erfolgt die Kontrolle über Berechtigungsgruppen und Passwortkennungen. Der Auftraggeber kann die Fernwartungen jederzeit einsehen, mitverfolgen und jederzeit abbrechen.

Verfügbarkeit und Belastbarkeit gemäß Art. 32 Abs. 1 DSGVO

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Die zufällige Zerstörung von personenbezogenen Daten ist geschützt durch:

- Einsatz von RAID Festplattensystemen
- Einsatz von USV inklusive redundanter Stromversorgung
- Serverüberwachungssystem über externes Systemhaus
- Tägliche inkrementelle Datenbanksicherungen; Vater-Sohn-Enkel
- Doppelte Veeam Datensicherungen, sowohl im Haus wie auch extern
-

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

Datenschutzmanagement

Der Auftragnehmer ist gesetzlich nicht verpflichtet, einen externen Datenschutzbeauftragten zu bestellen. Trotzdem wird dem Auftraggeber garantiert, dass sich der Auftragnehmer an die Einhaltung der DSGVO Datenschutzregeln hält und er seine Mitarbeiter regelmäßig schult.

Incident-Response-Management

Server und System werden von einem externen Dienstleister überwacht. Eine Meldung von Sicherheitsvorfällen an den Auftragnehmer erfolgt unverzüglich.

Datenschutzfreundliche Voreinstellungen; Art. 25 Abs. 2

Grundsätzlich werden nur Daten erhoben und verarbeitet, welche für die Geschäftszwecke erforderlich sind. Der Auftragnehmer ist lediglich Dienstleister im Bereich der Implementierung, Umsetzung, Projektierung und Support von Softwareprodukten der Sage Software GmbH und nicht für die Konzeption bzw. die Entwicklung der Sage Softwareprodukte verantwortlich. Bei Gestaltung, Umsetzung, Implementierung und Support handelt der Auftragnehmer ausschließlich nach Vorgabe der Kunden.

Auftragskontrolle

Alle Mitarbeiter des Auftragnehmers kennen den Datenverarbeitungszweck. Sie erhalten regelmäßige Weisungen zum Umgang mit personenbezogenen Daten und werden darauf schriftlich verpflichtet. Spezielle Unterauftragsverhältnisse werden schriftlich beauftragt.

Anlage 3
Unterauftragnehmer

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	Sage GmbH
Adresse	Franklinstraße 61-63 60486 Frankfurt/Main, Deutschland
Telefonnummer; E-Mail	069 / 50007-0; info@sage.de
Ansprechpartner	Geschäftsführer: Heino Erdmann
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	3rd Level Support für das in Anlage 1 genannte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump / Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	Systemhaus Tröndle GmbH
Adresse	Josef-Schüttler-Straße 53 78224 Singen, Deutschland
Telefonnummer; E-Mail	07731 / 167300-0, info@troendle.de
Ansprechpartner	Geschäftsführer: Dipl. Informatiker (FH) Stefan Tröndle
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	3rd Level Support für das in Anlage 1 genannte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump / Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	Skyfillers GmbH
Adresse	Schiffbrücke 66 24939 Flensburg, Deutschland
Telefonnummer; E-Mail	0461 / 404810-00; info@skyfillers.com
Ansprechpartner	Geschäftsführer: Jörg Hennemann
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	Bereitstellung von Cloud- und Hosting-Diensten, insbesondere Microsoft Exchange Hosting, Managed Spamfilterservice sowie E-Mail-Archivierung.

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	O & S EDV GmbH
Adresse	Stettiner Str. 7 88250 Weingarten, Deutschland
Telefonnummer; E-Mail	0751 / 361660; info@osedv.de
Ansprechpartner	Geschäftsführer: Margot Sterk, Daniel Sterk
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	Programmierungen und Anpassungen von Auswertungen rund um die Sage Software, insbesondere der Sage 100, Sage Office Line und Sage CRM.

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	IAS Vollmond
Adresse	Alfred Nobel Allee 41 66793 Saarwellingen, Deutschland
Telefonnummer; E-Mail	06838-9794970; info@ias-web.de
Ansprechpartner	Geschäftsführer Herr Lutz
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	Lieferung und Unterstützung von Sage Softwarezusatzlösungen

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	Sellmore GmbH
Adresse	Am Brauhaus 5 01099 Dresden, Deutschland
Telefonnummer; E-Mail	0351 / 8967110; info@sellmore.de
Ansprechpartner	Herr Kaufmann
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	Lieferung, Unterstützung und Programmierung von Sage Zusatzlösungen

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	Pfleiderer IT
Adresse	Schlehenweg 7 74259 Widdern, Deutschland
Telefonnummer; E-Mail	07943 / 9438632
Ansprechpartner	Herr Rüdiger Pfleiderer
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	Sage Consulting

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	LogiSoft GmbH & Co. KG
Adresse	Maybachstr. 7 35683 Dillenburg, BRD
Telefonnummer; E-Mail	02772 / 57269-0; info@logisoft.de
Ansprechpartner	Herr GF Tscherwitschke
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	Lieferung, Programmierung und Unterstützung Sage Aufgabencenter

Der Auftraggeber stimmt mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgenden Unterauftragnehmer (Subunternehmer) im Rahmen seiner Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	FTAPI Software GmbH
Adresse	Steinerstr. 15 f 81369 München, Deutschland
Telefonnummer; E-Mail	089 / 23069540; info@ftapi.de
Ansprechpartner	
Der Subunternehmer unterstützt in diesen Datenverarbeitungstätigkeiten	FTAPI ist eine Softwarelösung für Unternehmen, um große Dateien einfach, verschlüsselt, sicher und nachvollziehbar mit Partnern auszutauschen und zu speichern.