ALLGEMEINE GESCHÄFTSBEDINGUNGEN FÜR osapiens CLOUD-SERVICES („AGB")

1. BEGRIFFSBESTIMMUNGEN

Großgeschriebene Begriffe, die in diesem Dokument verwendet werden, sind im Glossar definiert.

2. NUTZUNGSRECHTE UND BESCHRÄNKUNGEN

2.1 Gewährung von Rechten.

osapiens gewährt dem Kunden ein nicht ausschließliches, nicht übertragbares und weltweites Recht, den Cloud-Service (einschließlich seiner Implementierung und Konfiguration), die Cloud-Materialien und die Dokumentation ausschließlich für den internen Geschäftsbetrieb des Kunden und seiner verbundenen Unternehmen zu nutzen. Zulässige Nutzungen und Einschränkungen des Cloud-Service gelten auch für Cloud-Materialien und -Dokumentation.

2.2 Autorisierte Benutzer.

Der Kunde kann autorisierten Benutzern die Nutzung des Cloud-Service gestatten. Die Nutzung ist auf die im Bestellformular angegebenen Nutzungsmetriken und Volumina beschränkt. Die Zugangsdaten für den Cloud-Service dürfen nicht von mehr als einer Person genutzt werden, können aber von einer Person auf eine andere übertragen werden, wenn der ursprüngliche Nutzer den Cloud-Service nicht mehr nutzen darf. Der Kunde ist für Vertragsverletzungen verantwortlich, die von autorisierten Benutzern verursacht werden.

2.3 Richtlinie über die zulässige Nutzung.

In Bezug auf den Cloud-Service darf der Kunde:

(a) außer in dem Umfang, in dem auf diese Rechte nicht rechtsgültig verzichtet werden kann, keine Inhalte oder Daten disassemblieren, dekompilieren, zurückentwickeln, kopieren, übersetzen oder damit abgeleitete Werke erstellen

(b) oder übermitteln, die ungesetzlich sind oder geistige Eigentumsrechte verletzen, oder (c) dessen Betrieb oder Sicherheit umgehen oder gefährden.

2.4 Verifizierung der Verwendung.

Der Kunde muss seine eigene Nutzung des Cloud-Service überwachen und jede Nutzung, die die Nutzungsmetriken und das Volumen überschreitet, melden. osapiens kann die Nutzung überwachen, um die Einhaltung der Nutzungsmetriken, des Volumens und des Vertrags zu kontrollieren.

2.5 Unterbrechung des Cloud-Service.

osapiens kann die Nutzung des Cloud-Service aussetzen oder einschränken, wenn die fortgesetzte Nutzung dem Cloud-Service oder seinen Nutzern erheblichen Schaden zufügen kann. osapiens muss den Kunden unverzüglich über die Aussetzung oder Einschränkung informieren. osapiens muss eine Aussetzung oder Einschränkung zeitlich und im Umfang so begrenzen, wie es unter den gegebenen Umständen möglich ist.

2.6 Webdienste von Drittanbietern.

Der Cloud-Service kann Integrationen mit Webdiensten enthalten, die von Dritten (mit Ausnahme der verbundenen Unternehmen) zur Verfügung gestellt werden, auf die über den Cloud-Service zugegriffen wird und die den Bedingungen mit diesen Dritten unterliegen. Diese Webservices von Drittanbietern sind nicht Teil des Cloud-Service und der Vertrag gilt nicht für sie.

2.7 Mobiler Zugriff auf den Cloud-Service.

Autorisierte Benutzer können auf bestimmte Cloud-Services über mobile Anwendungen zugreifen, die sie von Websites Dritter wie dem Android- oder Apple-App-Store erhalten. Die Nutzung mobiler Anwendungen kann durch die Bedingungen geregelt werden, die beim Herunterladen/Zugriff auf die mobile Anwendung präsentiert werden, und nicht durch die Bedingungen des Vertrags.

2.8 Vor-Ort-Komponenten.

Der Cloud-Service kann Vor-Ort--Komponenten enthalten, die vom Kunden heruntergeladen und installiert werden können (einschließlich Updates). Das Software Service Availability SLA gilt nicht für diese Komponenten.

3. OSAPIENS VERANTWORTLICHKEITEN

3.1 Bereitstellung.

osapiens stellt den Zugang zum Cloud-Service wie im Vertrag beschrieben zur Verfügung.

3.2 Unterstützung.

osapiens bietet Support für den Cloud-Service, wie im Bestellformular beschrieben.

3.3 Sicherheit.

osapiens muss angemessene technische und organisatorische Maßnahmen ergreifen und aufrechterhalten, um die von osapiens im Rahmen des Cloud-Service verarbeiteten personenbezogenen Daten, wie in der in das Bestellformular aufgenommenen Datenverarbeitungsvereinbarung für osapiens Cloud-Services beschrieben, gemäß dem geltenden Datenschutzrecht schützen.

3.4 Modifikationen.

(a) Der Cloud-Service und die Richtlinien von osapiens können von osapiens geändert werden. osapiens muss den Kunden per E-Mail, über das Support-Portal, die Versionshinweise, die Dokumentation oder den Cloud-Service über Änderungen informieren. Die Informationen werden per E-Mail zugestellt, wenn es sich bei der Änderung nicht nur um eine Erweiterung handelt. Änderungen können optionale neue Funktionen für den Cloud-Service enthalten, die der Kunde vorbehaltlich der jeweils aktuellen Ergänzung und Dokumentation nutzen kann.

(b) Stellt der Kunde fest, dass eine Änderung nicht nur eine Verbesserung darstellt und den Cloud-Service erheblich einschränkt, kann er seine Abonnements für den betroffenen Cloud-Service durch schriftliche Mitteilung an osapiens innerhalb von dreißig Tagen nach Erhalt der Informationsmitteilung von osapiens kündigen.

3.5 Analysen und Verbesserungen des Cloud-Service.

osapiens und die verbundenen Unternehmen von osapiens sind berechtigt, die Daten des Kunden und die aus der Nutzung des Cloud-Service und der Beratungsdienste durch den Kunden abgeleiteten Informationen zu verwenden, um Analysen zu erstellen, wie nachstehend dargelegt („**Analysen**"), und auf Grundlage der Analysen den Cloud-Service weiter zu verbessern, Korrelationen aus den Daten des Kunden abzuleiten und den anschließend verbesserten Cloud-Service nach eigenem Ermessen zu nutzen. Die Analysen werden Informationen anonymisiert sammeln, sie enthalten also weder Kundendaten noch personenbezogene Daten und werden als Cloud-Materialien behandelt. Die Kundendaten werden nicht an Dritte weitergegeben und der Kunde bleibt Eigentümer der Kundendaten.

Die Analysen können für folgende Zwecke verwendet werden:

(a) Produktverbesserung (insbesondere Produktmerkmale und -funktionalität, Arbeitsabläufe und Benutzeroberflächen) und Entwicklung neuer osapiens-Produkte und -Dienstleistungen,

(b) Verbesserung der Ressourcenzuweisung und Unterstützung,

(c) interne Bedarfsplanung,

(d) Training und Entwicklung von Algorithmen für maschinelles Lernen,

(e) Verbesserung der Produktleistung,
(f) Überprüfung der Sicherheit und Datenintegrität
(g) Identifizierung von Branchentrends und -entwicklungen, Erstellung von Indizes und anonymes Benchmarking.
(h) Auffinden von Mustern und Korrelationen für Zwecke der künstlichen Intelligenz

Soweit nicht anders vereinbart, werden die in den Kundendaten enthaltenen personenbezogenen Daten nur zur Erbringung des Cloud-Service und der Beratungsleistungen nach Maßgabe dieser AGB verwendet.

4. KUNDEN- UND PERSONENBEZOGENE DATEN

4.1 Kundendaten.

Der Kunde ist für die Kundendaten und deren Eingabe in den Cloud-Service verantwortlich. Der Kunde gewährt osapiens (einschließlich seiner verbundenen Unternehmen und Unterauftragnehmer) ein nicht ausschließliches Recht zur Verarbeitung von Kundendaten ausschließlich zur Bereitstellung und Unterstützung des Cloud-Service.

4.2 Personenbezogene Daten.

Der Kunde wird alle in den Kundendaten enthaltenen personenbezogenen Daten gemäß den geltenden Datenschutzgesetzen erfassen und pflegen.

4.3 Sicherheit.

Der Kunde muss angemessene Sicherheitsstandards für die Nutzung des Cloud-Service durch seine autorisierten Benutzer einhalten. Der Kunde darf ohne vorherige Zustimmung von osapiens keine Penetrationstests des Cloud-Service durchführen oder autorisieren.

4.4 Zugriff auf Kundendaten.

(a) Während der Abonnementlaufzeit kann der Kunde jederzeit auf seine Kundendaten zugreifen.
(b) Vor Ablauf der Abonnementlaufzeit kann der Kunde die Self-Service-Export-Tools von osapiens (soweit verfügbar) nutzen, um einen endgültigen Export der Kundendaten aus dem Cloud-Service durchzuführen.
(c) Bei Beendigung des Vertrags muss osapiens die auf den Servern, die den Cloud-Service hosten, verbleibenden Kundendaten löschen, es sei denn, das anwendbare Recht schreibt eine Aufbewahrung vor. Die aufbewahrten Daten unterliegen den Vertraulichkeitsbestimmungen des Vertrags.
(d) Im Falle eines Rechtsstreits mit Dritten, der sich auf die Kundendaten bezieht, muss osapiens in Bezug auf den Umgang mit den Kundendaten mit dem Kunden kooperieren und geltendes Recht einhalten (beides auf Kosten des Kunden).

5. GEBÜHREN UND STEUERN

5.1 Gebühren und Bezahlung.

Der Kunde muss die Gebühren wie im Bestellformular angegeben bezahlen. Nach vorheriger schriftlicher Ankündigung kann osapiens die Nutzung des Cloud-Service durch den Kunden bis zur Zahlung aussetzen. Der Kunde kann während der Abonnementlaufzeit weder geschuldete Gebühren zurückhalten, reduzieren oder aufrechnen noch Nutzungsmetriken reduzieren. Alle Bestellformulare sind nicht stornierbar und die Gebühren werden nicht zurückerstattet.

5.2 Steuern.

Gebühren und andere Kosten, die im Rahmen eines Bestellformulars erhoben werden, enthalten keine Steuern, die alle auf Rechnung des Kunden gehen. Der Kunde ist für alle Steuern verantwortlich, mit Ausnahme der Einkommens- und Lohnsteuer von osapiens. Der Kunde muss

osapiens alle Direktzahlungsgenehmigungen oder gültigen Steuerbefreiungsbescheinigungen zur Verfügung stellen, bevor er ein Auftragsformular unterzeichnet. Falls osapiens zur Zahlung von Steuern (mit Ausnahme der Einkommens- und Lohnsteuer) verpflichtet ist, muss der Kunde osapiens diese Beträge erstatten und osapiens von allen Steuern und damit zusammenhängenden Kosten freistellen, die von osapiens aufgrund dieser Steuern gezahlt wurden oder zu zahlen sind.

6. LAUFZEIT UND KÜNDIGUNG

6.1 Laufzeit.

Die Laufzeit des Abonnements ist wie im Bestellformular angegeben.

6.2 Kündigung.

Eine Partei kann den Vertrag kündigen:

(a) nach einer schriftlichen Benachrichtigung 30 Tage im Vorhinein über eine wesentliche Verletzung durch die andere Partei, es sei denn, die Verletzung wird innerhalb dieser dreißigtägigen Frist beseitigt

(b) wie gemäß den Abschnitten 3.4 (b), 7.3 (b), 7.4 (c) oder 8.1 (c) zulässig (wobei die Kündigung in jedem dieser Fälle dreißig Tage nach Erhalt der Mitteilung wirksam wird), oder

(c) vorbehaltlich des anwendbaren Rechts, unverzüglich, wenn die andere Partei Konkurs anmeldet, zahlungsunfähig wird, eine Abtretung zugunsten der Gläubiger vornimmt oder anderweitig wesentlich gegen die Abschnitte 11 oder 12.6 verstößt.

6.3 Rückerstattung und Zahlungen.

Bei einer Kündigung durch den Kunden oder einer Kündigung nach 8.1(c) ist der Kunde berechtigt:

(a) eine anteilige Rückerstattung in Höhe des ungenutzten Anteils der im Voraus bezahlten Gebühren für das gekündigte Abonnement, berechnet ab dem Datum der effektiven Kündigung, und

(b) eine Befreiung von der Verpflichtung zur Zahlung fälliger Gebühren für Zeiträume nach dem Wirksamkeitsdatum der Kündigung zu erhalten.

6.4 Auswirkungen des Ablaufs oder der Kündigung.

Nach Inkrafttreten des Ablaufs oder der Kündigung des Vertrags:

(a) endet das Recht des Kunden zur Nutzung des Cloud-Service und aller vertraulichen Informationen von osapiens,

(b) müssen vertrauliche Informationen der offenlegenden Partei gemäß dem Vertrag zurückgegeben oder vernichtet werden, wobei

(c) die Kündigung oder der Ablauf des Vertrags keine anderen Vereinbarungen zwischen den Parteien berührt.

6.5 Fortbestand.

Die Abschnitte 1, 5, 6.3, 6.4, 6.5, 8, 9, 10, 11 und 12 überdauern den Ablauf oder die Kündigung des Vertrags.

7. GARANTIEN

7.1 Einhaltung von Gesetzen.

Jede Partei garantiert die aktuelle und fortwährende Einhaltung aller für sie geltenden Gesetze und Vorschriften im Zusammenhang mit:

(a) im Fall von osapiens, dem Betrieb des Geschäfts von osapiens, soweit es sich auf den Cloud-Service bezieht, und (b) im Fall des Kunden, den Kundendaten und der Nutzung des Cloud-Service durch den Kunden.

7.2 Gute Industriepraktiken.

osapiens gewährleistet, dass es den Cloud-Service wie folgt zur Verfügung stellt:

(a) im Wesentlichen gemäß der Dokumentation; und

(b) mit dem Maß an Fachkenntnis und Sorgfalt, das vernünftigerweise von einem qualifizierten und erfahrenen globalen Anbieter von Dienstleistungen erwartet werden kann, die der Art und Komplexität des Cloud-Service im Wesentlichen entsprechen.

7.3 Rechtsmittel.

Die einzigen und ausschließlichen Rechtsmittel des Kunden und die gesamte Haftung von osapiens für die Verletzung der Garantie gemäß Abschnitt 7.2 sind:

(a) die Wiederherstellung des mangelhaften Cloud-Service, und

(b) wenn osapiens die Nacherfüllung nicht vornimmt, kann der Kunde sein Abonnement für den betroffenen Cloud-Service kündigen. Eine Kündigung muss innerhalb von drei Monaten nach der Nichterfüllung durch osapiens erfolgen.

7.4 Software-Service-Verfügbarkeit.

(a) osapiens gewährleistet die Aufrechterhaltung einer durchschnittlichen monatlichen Software-Service-Verfügbarkeit für das Produktionssystem des Cloud-Service, wie sie in der jeweiligen Service-Level-Vereinbarung oder Ergänzung („SLA") definiert ist.

(b) Das einzige und ausschließliche Rechtsmittel des Kunden bei einer Verletzung der SLA durch osapiens ist die Ausstellung einer Gutschrift in der in der SLA beschriebenen Höhe. Der Kunde muss das von osapiens bekannt gegebene Verfahren zur Beantragung von Gutschriften befolgen. Wenn die Gültigkeit der Service-Gutschrift von osapiens schriftlich bestätigt wird (E-Mail zulässig), kann der Kunde die Gutschrift auf eine zukünftige Rechnung für den Cloud-Service anrechnen lassen oder eine Rückerstattung des Gutschriftbetrags verlangen, wenn keine zukünftige Rechnung fällig ist.

(c) Für den Fall, dass osapiens die SLA (i) für vier aufeinanderfolgende Monate oder (ii) für fünf oder mehr Monate innerhalb eines Zwölfmonatszeitraums oder (iii) mit einer Software-Service-Verfügbarkeit von mindestens 95 % für einen Kalendermonat nicht einhält, kann der Kunde seine Abonnements für den betroffenen Cloud-Service kündigen, indem er osapiens innerhalb von dreißig Tagen nach der Nichterfüllung eine schriftliche Mitteilung übermittelt.

7.5 Gewährleistungsausschlüsse.

Die Garantien in den Abschnitten 7.2 und 7.4 gelten nicht, wenn:

(a) der Cloud-Dienst nicht gemäß dem Vertrag oder der Dokumentation genutzt wird,

(b) eine Nichtkonformität durch den Kunden, durch ein Produkt oder eine Dienstleistung verursacht wird, die nicht von osapiens bereitgestellt wurde, oder

(c) der Cloud-Dienst kostenlos zur Verfügung gestellt wurde.

7.6 Haftungsausschluss.

Sofern nicht ausdrücklich im Vertrag vorgesehen, geben weder osapiens noch seine Subunternehmer irgendwelche ausdrücklichen oder stillschweigenden, gesetzlichen oder anderweitigen Zusicherungen oder Garantien in Bezug auf irgendeine Angelegenheit, einschließlich der Marktgängigkeit, Eignung, Originalität oder Eignung für einen bestimmten Gebrauch oder Zweck, der Nichtverletzung von Rechten oder der Ergebnisse, die aus der Nutzung oder Integration von Produkten oder Dienstleistungen, die im Rahmen des Vertrags zur Verfügung gestellt werden, abgeleitet werden, oder dass der Betrieb von Produkten oder Dienstleistungen sicher, ununterbrochen oder fehlerfrei sein wird. Der Kunde erklärt sich damit einverstanden, dass er sich

beim Erwerb von Abonnements für einen Cloud-Service nicht auf die Lieferung zukünftiger Funktionen, öffentliche Kommentare oder Werbung von osapiens oder Produkt-Roadmaps verlässt.

8. ANSPRÜCHE DRITTER

8.1 Gegen den Kunden erhobene Ansprüche.

Falls ein Anspruch geltend gemacht wird oder wahrscheinlich geltend gemacht wird, kann osapiens (i) dem Kunden das Recht verschaffen, den Cloud-Service gemäß den Bedingungen des Vertrags weiter zu nutzen, oder (ii) den Cloud-Service ersetzen oder abändern, so dass er keine Verletzung mehr darstellt, ohne dass eine wesentliche Verringerung der Funktionalität eintritt. Wenn diese Optionen nicht in zumutbarer Weise verfügbar sind, können osapiens oder der Kunde das Abonnement des Kunden für den betroffenen Cloud-Service durch schriftliche Mitteilung an die jeweils andere Seite kündigen.

8.2 Gegen osapiens erhobene Ansprüche.

Der Kunde muss osapiens gegen Ansprüche verteidigen, die von Dritten im Zusammenhang mit Kundendaten gegen osapiens, seine verbundenen Unternehmen und Unterauftragnehmer erhoben werden.

9. HAFTUNGSBESCHRÄNKUNG

9.1 Unbeschränkte Haftung.

Keine der beiden Parteien schließt ihre Haftung für Schäden aus, die sich aus folgenden Sachverhalten ergeben:

(a) der Verpflichtungen der Parteien gemäß Abschnitt 8.1(a) und 8.2,

(b) der unbefugten Nutzung oder Offenlegung vertraulicher Informationen,

(c) der Verletzung der Datenschutz- und Sicherheitspflichten durch eine der Parteien, die zu einer unbefugten Nutzung oder Offenlegung personenbezogener Daten führt,

(d) grober Fahrlässigkeit oder vorsätzlichem Fehlverhalten, oder

(e) jedem Versäumnis des Kunden, fällige Gebühren aus dem Vertrag zu zahlen.

9.2 Haftungsobergrenze.

Vorbehaltlich der Ziffern 9.1 und 9.3 darf die maximale Gesamthaftung einer der Parteien (oder ihrer jeweiligen verbundenen Unternehmen oder der Subunternehmer von osapiens) gegenüber der anderen Partei oder einer anderen natürlichen oder juristischen Person für alle Ereignisse (oder eine Reihe von zusammenhängenden Ereignissen), die in einem Zeitraum von zwölf Monaten auftreten, nicht die jährlichen Abonnementgebühren übersteigen, die für den jeweiligen Cloud-Service, der den Schaden direkt verursacht hat, in diesem Zeitraum von zwölf Monaten gezahlt wurden. Jeder „Zwölf-Monats-Zeitraum" beginnt mit dem Startdatum der Abonnementlaufzeit oder einem ihrer Jahrestage.

9.3 Ausschluss von Schadensersatz. Vorbehaltlich von Abschnitt 9.1:

(a) haftet keine der Parteien (und auch nicht ihre jeweiligen verbundenen Unternehmen oder die Subunternehmer von osapiens) gegenüber der anderen Partei für Folgeschäden oder indirekte Schäden, den Verlust von Firmenwert oder Geschäftsgewinnen, Arbeitsunterbrechungen oder Strafschadensersatz, und

(b) osapiens haftet nicht für Schäden, die durch einen unentgeltlich zur Verfügung gestellten Cloud-Service entstehen.

9.4 Risikoallokation.

Der Vertrag regelt die Risikoverteilung zwischen osapiens und dem Kunden. Die Gebühren für den Cloud-Service und die Beratungsdienste spiegeln diese Risikoverteilung und Haftungsbeschränkung wider.

10. RECHTE AN GEISTIGEM EIGENTUM

10.1 Im Eigentum von osapiens.

osapiens sowie seine verbundenen Unternehmen oder Lizenzgeber sind Eigentümer aller geistigen Eigentumsrechte an und im Zusammenhang mit dem Cloud-Service, den Cloud-Materialien, der Dokumentation, den Beratungsleistungen, den Designbeiträgen, dem damit verbundenen Wissen oder Prozessen sowie allen davon abgeleiteten Werken. Alle Rechte, die dem Kunden nicht ausdrücklich gewährt werden, sind osapiens und seinen Lizenzgebern vorbehalten.

10.2 Kundeneigentum.

Der Kunde behält alle Rechte an und in Bezug auf die Kundendaten. osapiens darf die vom Kunden bereitgestellten Marken ausschließlich zur Bereitstellung und Unterstützung des Cloud-Service verwenden.

10.3 Nichtgeltendmachung von Rechten.

Der Kunde verpflichtet sich, im eigenen Namen und im Namen seiner Nachfolger und Abtretungsempfänger, keine Rechte oder Ansprüche auf Rechte an Cloud-Services, Cloud-Materialien, Dokumentationen oder Beratungsleistungen gegenüber osapiens, den damit verbundenen Unternehmen oder Lizenzgebern geltend zu machen.

11. VERTRAULICHKEIT

11.1 Verwendung von vertraulichen Informationen.

(a) Die empfangende Partei muss alle vertraulichen Informationen der offenlegenden Partei im gleichen Maße als streng vertraulich schützen, wie sie ihre eigenen vertraulichen Informationen schützt, und zwar nicht weniger als mit einem angemessenen Sorgfaltsstandard. Die empfangende Partei darf keine vertraulichen Informationen der offenlegenden Partei an andere Personen als ihre Mitarbeiter, Vertreter oder autorisierten Benutzer weitergeben, deren Zugang notwendig ist, um ihnen die Ausübung ihrer Rechte oder die Erfüllung ihrer Verpflichtungen aus dem Vertrag zu ermöglichen, und die im Wesentlichen ähnlichen Vertraulichkeitsverpflichtungen wie in Abschnitt 11 unterliegen. Der Kunde darf die Vereinbarung oder die Preisgestaltung nicht an Dritte bekanntgeben.

(b) Vertrauliche Informationen einer der beiden Parteien, die vor der Ausführung des Vertrags offengelegt wurden, unterliegen Abschnitt 11.

(c) Im Falle eines Gerichtsverfahrens in Bezug auf die vertraulichen Informationen, muss die empfangende Partei mit der offenlegenden Partei kooperieren und das anwendbare Recht in Bezug auf den Umgang mit den vertraulichen Informationen einhalten (alles auf Kosten der offenlegenden Partei).

11.2 Ausnahmen.

Die Beschränkungen bezüglich der Verwendung oder Offenlegung von vertraulichen Informationen gelten nicht für vertrauliche Informationen:

(a) die von der empfangenden Partei unabhängig und ohne Bezugnahme auf die vertraulichen Informationen der offenlegenden Partei entwickelt werden,

(b) die der Öffentlichkeit allgemein zugänglich ist, ohne dass die empfangende Partei den Vertrag verletzt hat,

(c) die zum Zeitpunkt der Offenlegung der empfangenden Partei ohne Vertraulichkeitsbeschränkungen bekannt waren, oder

(d) in Bezug auf welche die offenlegende Partei schriftlich zustimmt, dass sie frei von Vertraulichkeitsbeschränkungen sind.

11.3 Werbung.

Osapiens darf den Namen und das Logo des Kunden in Kundenlisten, auf der eigenen Webseite oder in vierteljährlichen Telefonaten mit seinen Investoren verwenden. Außerdem kann osapiens, wenn die Parteien dies vereinbaren, den Kunden im Rahmen von Marketingmaßnahmen einbeziehen (einschließlich von Referenzanrufen und -berichten, Presseberichten, Besuchen vor Ort oder Teilnahmen an Veranstaltungen von osapiens). Der Kunde erklärt sich damit einverstanden, dass osapiens hochrangige Informationen über den Kunden zu Marketing- und Schulungszwecken an seine verbundenen Unternehmen weitergeben darf.

12. VERSCHIEDENES

12.1 Trennbarkeit.

Sollte eine Bestimmung des Vertrags für ungültig oder nicht durchsetzbar erachtet werden, so berührt diese Ungültigkeit oder Nichtdurchsetzbarkeit die übrigen Bestimmungen des Vertrags nicht.

12.2 Kein Verzicht.

Ein Verzicht auf eine Vertragsverletzung gilt nicht als Verzicht auf eine andere Vertragsverletzung.

12.3 Elektronische Unterschrift.

Unterschriften in jeder elektronischen Form (einschließlich E-Mail oder dedizierte Signaturlösungen) gelten als Originalunterschriften.

12.4 Regulatorische Angelegenheiten.

Die vertraulichen Informationen von osapiens unterliegen den Exportkontrollgesetzen verschiedener Länder, einschließlich der Gesetze der Vereinigten Staaten und Deutschlands. Der Kunde darf die vertraulichen Informationen von osapiens keiner Regierungsbehörde zur Prüfung von Lizenzen oder anderen behördlichen Genehmigungen vorlegen und darf die vertraulichen Informationen von osapiens nicht in Länder, Personen oder an Unternehmen exportieren, wenn dies durch Exportgesetze verboten ist.

12.5 Mitteilungen.

Alle Mitteilungen müssen in schriftlicher Form erfolgen und an die in einem Bestellformular angegebene Adresse zugestellt werden. Mitteilungen von osapiens, die sich auf Betrieb oder Support des Cloud-Service beziehen, sowie solche gemäß den Abschnitten 3.4 und 5.1 können in Form einer elektronischen Mitteilung an den im Bestellformular angegebenen bevollmächtigten Vertreter oder Administrator des Kunden erfolgen.

12.6 Abtretung.

Ohne die vorherige schriftliche Zustimmung von osapiens ist der Kunde nicht berechtigt, den Vertrag (oder seine Rechte und Pflichten) an eine andere Partei abzutreten oder zu übertragen. osapiens ist berechtigt, den Vertrag an eines seiner verbundenen Unternehmen abzutreten.

12.7 Unterauftragsvergabe.

osapiens kann Teile des Cloud-Service oder der Beratungsleistungen an Dritte weitervergeben. osapiens ist für Vertragsverletzungen, die durch seine Subunternehmer verursacht werden, verantwortlich.

12.8 Verhältnis der Parteien zueinander.

Die Parteien sind unabhängige Vertragspartner, wobei durch den Vertrag kein Partnerschafts-, Franchise-, Joint-Venture-, Agentur-, Treuhand- oder Arbeitsverhältnis zwischen den Parteien entsteht.

12.9 Höhere Gewalt.

Jede Verzögerung der Leistungserbringung (mit Ausnahme der Zahlung fälliger Beträge), die durch Umstände verursacht wird, die außerhalb der zumutbaren Kontrolle der ausführenden Partei liegen, stellt keine Vertragsverletzung dar. Die Leistungsfrist verlängert sich um den Zeitraum, der der Dauer der Leistungshindernisse entspricht.

12.10 Geltendes Recht.

Dieser Vertrag und alle Ansprüche, die sich auf seinen Gegenstand beziehen, unterliegen ausschließlich dem Recht der Bundesrepublik Deutschland unter Ausschluss der Bestimmungen des UN-Kaufrechts (CISG) und des internationalen Privatrechts.
Ausschließlicher Gerichtsstand für alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag oder seiner Gültigkeit ergeben, ist Mannheim.

12.11 Gesamte Vereinbarung.

Der Vertrag stellt die vollständige und ausschließliche Vereinbarung zwischen osapiens und dem Kunden im Zusammenhang mit der Geschäftsbeziehung der Parteien in Bezug auf den Vertragsgegenstand dar. Alle früheren Zusicherungen, Besprechungen und Schriftstücke (einschließlich etwaiger Vertraulichkeitsvereinbarungen) sind im Vertrag aufgegangen und werden durch diesen ersetzt, und die Parteien lehnen jegliches Vertrauen in Bezug auf diese ab. Der Vertrag kann nur in schriftlicher Form mit Unterschrift beider Parteien geändert werden, außer wie in Abschnitt 3.4 gestattet. Eine Vereinbarung hat Vorrang vor den Bedingungen einer vom Kunden ausgestellten Bestellung, die keine Gültigkeit hat, auch wenn osapiens die Bestellung annimmt oder nicht anderweitig ablehnt.

Glossar

1.1 „Verbundenes Unternehmen" einer Partei ist jede juristische Person, an der eine Partei direkt oder indirekt mehr als fünfzig Prozent (50 %) ihrer Anteile oder Stimmrechte hält. Jede juristische Person wird als verbundenes Unternehmen betrachtet, solange diese Beteiligung aufrechterhalten wird.

1.2 „Vertrag" bedeutet ein Bestellformular und in ein Bestellformular aufgenommene Dokumente.

1.3 „Autorisierter Benutzer" bezeichnet jede Person, der der Kunde eine Zugangsberechtigung zur Nutzung des Cloud-Service erteilt, die ein Mitarbeiter, Agent, Auftragnehmer oder Vertreter des

(a) Kunden,

(b) der mit dem Kunden verbundenen Unternehmen, bzw.

(c) der Geschäftspartner des Kunden und der verbundenen Unternehmen des Kunden ist.

1.4 „Geschäftspartner" bezeichnet eine juristische Person, die die Nutzung eines Cloud-Service in Verbindung mit dem internen Geschäftsbetrieb des Kunden und seiner verbundenen Unternehmen benötigt. Dazu können Kunden, Vertriebspartner, Dienstleister bzw. Lieferanten des Kunden gehören.

1.5 „Cloud-Service" bezeichnet jede eigenständige, abonnementbasierte, gehostete, unterstützte und betriebene On-Demand-Lösung, die von osapiens im Rahmen eines Auftragsformulars bereitgestellt wird.

1.6 „Cloud-Materialien" sind alle Materialien, die von osapiens (selbständig oder unter Mitwirkung des Kunden) im Rahmen der Erfüllung des Vertrags bereitgestellt oder entwickelt werden, auch bei der Erbringung von Support- oder Beratungsleistungen für den Kunden. Zu den Cloud-Materialien gehören weder die Kundendaten, noch vertrauliche Informationen des Kunden oder der Cloud-Service.

1.7 „Vertrauliche Informationen" bedeutet

(a) in Bezug auf den Kunden: (i) die Kundendaten, (ii) die Marketing- und Geschäftsanforderungen des Kunden, (iii) die Implementierungspläne des Kunden bzw. (iv) die Finanzinformationen des Kunden, und

(b) in Bezug auf osapiens: (i) den Cloud-Service, die Dokumentation, die Cloud-Materialien und die Analysen gemäß Abschnitt 3.5 und (ii) Informationen über die Forschung und Entwicklung von osapiens, Produktangebote, Preise und Verfügbarkeit.

(c) Zu den vertraulichen Informationen von osapiens oder des Kunden gehören auch Informationen, die die offenlegende Partei vor uneingeschränkter Offenlegung gegenüber anderen schützt, die (i) von der offenlegenden Partei oder ihren Vertretern zum Zeitpunkt der Offenlegung als vertraulich bezeichnet werden oder (ii) angesichts der Art der Informationen und der Umstände ihrer Offenlegung vernünftigerweise als vertraulich angesehen werden sollten.

1.8 „Beratungsdienstleistungen" sind professionelle Dienstleistungen, wie z. B. Implementierung, Konfiguration, kundenspezifische Entwicklung und Schulung, die von Mitarbeitern oder Subunternehmern von osapiens erbracht werden, wie in einem Auftragsformular beschrieben, und die durch den Zusatz für Beratungsdienstleistungen oder eine ähnliche Vereinbarung geregelt sind.

1.9 „Kundendaten" sind alle Inhalte, Materialien, Daten und Informationen, die berechtigte Nutzer in das Produktionssystem eines Cloud-Service eingeben oder die der Kunde aus seiner Nutzung ableitet und im Cloud-Service speichert (z. B. kundenspezifische Berichte). Die Kundendaten und ihre Derivate enthalten keine vertraulichen Informationen von osapiens.

1.10 „Dokumentation" bezeichnet die zum jeweiligen Zeitpunkt aktuelle technische und funktionale Dokumentation von osapiens sowie ggf. Rollen- und Verantwortungsbeschreibungen für den Cloud-Service, die dem Kunden mit dem Cloud-Service zur Verfügung gestellt werden.

1.11 „Bestellformular" bezeichnet das Bestelldokument für einen Cloud-Service, das auf die AGB verweist.

1.12 „osapiens-Richtlinien" bezeichnen die von osapiens zur Bereitstellung und Unterstützung des Cloud-Service angewandten betrieblichen Richtlinien und Grundsätze, wie sie in einem Bestellformular enthalten sind.

1.13 „Abonnementlaufzeit" bezeichnet die im jeweiligen Bestellformular angegebene Laufzeit eines Cloud-Service-Abonnements, einschließlich aller Verlängerungen.

1.14 „Nachtrag" bezeichnet die ergänzenden Bedingungen, die für den Cloud-Service gelten und die in ein Bestellformular aufgenommen werden.

1.15 „Nutzungsmetrik" bezeichnet den Messstandard zur Bestimmung der zulässigen Nutzung und zur Berechnung der fälligen Gebühren für einen Cloud-Service, wie er in einem Bestellformular festgelegt ist.

SLA und SUPPORT-RICHTLINIE für osapiens CLOUD-SERVICES

Diese SLA- und Support-Richtlinie für osapiens Cloud-Services ist Teil einer Vereinbarung für bestimmte osapiens Cloud-Services („Vereinbarung") zwischen osapiens und dem Kunden.

BEGRIFFSBESTIMMUNGEN

1,1. **„Gutschrift"** bedeutet 2 % der vierteljährlichen Abonnementgebühren für jedes Prozent unter dem Systemverfügbarkeits-SLA, höchstens jedoch 100 % der monatlichen Abonnementgebühren.

1,2. **„Ausfallzeit"** bezeichnet die Gesamtheit der Minuten in einem Monat, in denen die Produktionsversion des Cloud-Service nicht verfügbar ist, mit Ausnahme der ausgeschlossenen Ausfallzeiten.

1,3. **„Ausgeschlossene Ausfallzeit"** bezeichnet die Gesamtminuten pro Monat, die einem Wartungsfenster oder einem größeren Upgrade-Fenster, für das der Kunde mindestens 48 Stunden im Voraus benachrichtigt wurde, oder einer Nichtverfügbarkeit aufgrund **höherer Gewalt** zuzuschreiben sind.

1,4. „**Ereignisse höherer Gewalt"** bezeichnet Faktoren, die außerhalb der zumutbaren Kontrolle von osapiens liegen und die auch bei Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können.

1,5. „**Wartungsfenster"** bezeichnet das wöchentliche Wartungsfenster für den Cloud-Service https://support.osapiens.com osapiens kann das Wartungsfenster von Zeit zu Zeit gemäß dem Vertrag aktualisieren.

1,6. **„Haupt-Upgrade-Fenster"** bezeichnet die erweiterten Upgrade-Wartungsfenster für den Cloud-Service gemäß https://support.osapiens.com osapiens kann das Haupt-Upgrade-Fenster von Zeit zu Zeit gemäß dem Vertrag aktualisieren.

1,7. „**Monat"** bedeutet einen Kalendermonat.

1,8. „Quartal" bezeichnet jeden Kalenderzeitraum von 3 aufeinanderfolgenden Monaten, beginnend am 1. Januar, 1. April, 1. Juli und 1. Oktober.

1,9. **„Monatliche Abonnementgebühren"** bezeichnet die monatlichen (oder 1/12 der jährlichen) Abonnementgebühren, die für den jeweiligen Cloud-Service gezahlt wurden, der das Systemverfügbarkeits-SLA nicht erfüllt hat.

1,10. Der **„Prozentsatz der Systemverfügbarkeit"** wird wie folgt berechnet und definiert:

$$\left(\frac{\text{Total Minutes in the Quarter - Excluded Downtime - Downtime}}{\text{Total Minutes in the Quarter - Excluded Downtime}}\right) *100$$

1,11. **„Systemverfügbarkeits-SLA"** bedeutet eine durchschnittliche Systemverfügbarkeit von 99,5 % (Standard) oder 99,8 % (Erweitert) in jedem Quartal für die Produktionsversion des Cloud-Service.

1,12. **„Gesamte Minuten pro Quartal"** werden 24 Stunden an 7 Tagen in der Woche während eines Quartals gemessen.

1,13. **„UTC"** bezeichnet den Standard der koordinierten Weltzeit, der die Startzeit für das jeweilige Wartungsfenster und das Haupt-Upgrade-Fenster darstellt.

SYSTEMVERFÜGBARKEITS-SLA UND GUTSCHRIFTEN

2,1. Gutschrift

Wenn osapiens die Systemverfügbarkeits-SLA für ein bestimmtes Quartal nicht erfüllt, kann der Kunde eine Gutschrift beantragen, die er auf eine künftige Rechnung für den Cloud-Service, der

die Systemverfügbarkeits-SLA nicht erfüllt hat, anrechnen lassen kann (vorbehaltlich der nachfolgenden Abschnitte 2.1.1 und 2.1.2).

2.1.1. Ansprüche auf eine Gutschrift müssen in gutem Glauben und durch eine dokumentierte Einreichung eines Supportfalls innerhalb von dreißig (30) Werktagen nach dem Ende des betreffenden Quartals, in dem osapiens die Systemverfügbarkeits-SLA für den Cloud-Service nicht erfüllt hat, geltend gemacht werden.

2.1.2. Kunden, die den Cloud-Service nicht direkt bei osapiens abonniert haben, müssen die Gutschrift bei ihrem jeweiligen osapiens-Partner beantragen.

2,2. Systemverfügbarkeitsbericht

osapiens muss dem Kunden einen monatlichen Bericht mit der Liste der Ausfallzeiten in Bezug auf den Prozentsatz der Systemverfügbarkeit für den Cloud-Service zur Verfügung stellen, und zwar entweder per E-Mail nach einer Anfrage an den dem Kunden zugewiesenen osapiens-Kundenbetreuer, über den Cloud-Service oder über ein dem Kunden zur Verfügung gestelltes Online-Portal, sofern und sobald ein solches Online-Portal verfügbar ist.

ÄNDERUNGEN DER WARTUNGSFENSTER

3,1. Wenn der Kunde über Änderungen der Wartungs- und Major-Upgrade-Fenster benachrichtigt werden möchte, muss er sich für den Erhalt von Benachrichtigungen unter support.osapiens.com anmelden.

SUPPORT-RICHTLINIE FÜR DIENSTLEISTUNGEN

osapiens bietet die folgenden Support-Levels an: osapiens Standard Support und osapiens Extended Support. Der osapiens Standard Support ist in den im Bestellformular angegebenen Abonnementgebühren für die osapiens Cloud Services enthalten.

Der osapiens Extended Support wird gegen eine zusätzliche Gebühr oder als Zusatz zum osapiens Standard Support für bestimmte osapiens Cloud Services angeboten. osapiens Extended Support ist nicht verfügbar und wird nicht für über osapiens erworbene Cloud-Services von Drittanbietern angeboten.

SYSTEMVERFÜGBARKEIT

osapiens garantiert dem Kunden eine durchschnittliche Verfügbarkeit des Cloud-Service gemäß dem Vertrag. Die durchschnittliche Systemverfügbarkeit wird in jedem Kalenderquartal gemessen.

	Standard Support	**Extended Support**
Systemverfügbarkeit SLA	99,5%	99,8%

VERFÜGBARKEIT VON SUPPORTLEISTUNGEN

Erste Reaktionszeiten werden nur während der Supportzeiten gemessen.

	Standard Support	**Extended Support**
Support-Zeiten	Montag – Freitag, 8:00 – 18:00 Uhr (Zeitzone DE/Berlin)	Montag – Sonntag, 24 Stunden "24x7"

Primäre Supportsprache ist Englisch.

Für private Cloud-Instanzen erwarten wir einen ssh-Zugang zum Server und einen Zugriff auf die Webapplikation (über Internet oder OpenVPN). Sind diese Voraussetzungen nicht gegeben, hat dies Einfluss auf die in der SLA genannte Reaktionszeit.

EINREICHEN VON SUPPORTANFRAGEN

Die vom Kunden benannte Kontaktperson muss Supportanfragen gemäß den Ticketing-Richtlinien von osapiens einreichen. Die Supportanfrage sollte einen Schweregrad gemäß dem nächsten Abschnitt zuweisen und den gemeldeten Fehler ausreichend beschreiben und dokumentieren, damit er behoben werden kann.

Support-Anfragen sind vom kundeneigenen Benutzer im osapiens Support-Portal einzureichen, um sicherzustellen, dass korrekte SLAs angewendet werden können.

osapiens kann den Schweregrad bei Vorliegen eines triftigen geschäftlichen Grundes oder wenn der Kunde nicht innerhalb der vereinbarten Reaktionszeiten reagiert, neu einstufen.

SCHWEREGRAD

osapiens reagiert auf eingereichte Support-Anfragen (auch als „Fall", „Vorfall" oder „Problem" bezeichnet) wie in unten stehender Tabelle beschrieben. Der Schweregrad bedeutet, dass ein wahrgenommener Fehler im osapiens Cloud Service die in der folgenden Tabelle angegebenen Auswirkungen hat.

Die erste Reaktionszeit beginnt, wenn der Kunde eine Support-Anfrage in ordnungsgemäßer Form im osapiens Support-Portal einreicht. Supportanfragen, die außerhalb der vereinbarten Supportzeiten eingehen, werden zu Beginn des nächsten Supportzeitfensters bearbeitet. Die erste Reaktionszeit endet mit der Bestätigung bzw. Lösung der Support-Anfrage oder dem Beginn der technischen Analyse und Interaktion mit dem Kunden. Osapiens verpflichtet sich zu den folgenden Antwortzeiten.

Die Reaktionszeiten sind abhängig vom Systemzugriff des Kunden in Echtzeit.

Priorität	Definition	Reaktionslevel
P1	**Sehr hoch:** Ein Vorfall sollte mit der Priorität „sehr hoch" eingestuft werden, wenn das Problem sehr schwerwiegende Folgen für normale Geschäftsprozesse oder IT-Prozesse hat, die mit Kerngeschäftsprozessen zusammenhängen. Dringende Arbeiten können nicht durchgeführt werden . Dies wird im Allgemeinen durch die folgenden Umstände verursacht: - Ein produktiver Dienst ist komplett ausgefallen.	**Erste Reaktion:** Innerhalb von zwei Stunden nach Übermittlung des Falls für Standard Support oder innerhalb einer Stunde für Extended Support. **Laufende Kommunikation:** Wenn nicht anders vom osapiens-Support mitgeteilt, einmal pro Stunde. **Lösungsziel:** osapiens stellt für Probleme entweder (i) eine Lösung oder (ii) eine Abhilfe oder (iii) einen Aktionsplan innerhalb von acht Stunden für den Standard Support oder innerhalb

	- Das bevorstehende System Go-Live oder Upgrade eines Produktionssystems kann nicht abgeschlossen werden. - Die Kerngeschäftsprozesse des Kunden sind stark betroffen. Es ist nicht für jeden Fall eine Abhilfe verfügbar. Der Vorfall erfordert eine sofortige Bearbeitung, da die Fehlfunktion ernsthafte Probleme verursachen kann.	von vier Stunden für Extended-Support-Kunden bereit.
P2	**Hoch:** Ein Vorfall sollte mit der Priorität „hoch" eingestuft werden, wenn normale Geschäftsprozesse ernsthaft betroffen sind. Notwendige Aufgaben können nicht ausgeführt werden. Dies wird durch fehlerhafte Funktionen im Cloud-Service verursacht, die sofort benötigt werden. Der Vorfall ist so schnell wie möglich zu bearbeiten, da eine anhaltende Störung den gesamten produktiven Geschäftsablauf empfindlich stören kann.	**Erste Reaktion:** Innerhalb von acht Stunden nach Einreichung des Falls für den Standard Support oder innerhalb von vier Stunden nach Einreichung des Falls für Extended-Support-Kunden. **Laufende Kommunikation:** Wenn nicht anders von osapiens mitgeteilt, einmal alle sechs Stunden. **Lösungsziel:** osapiens stellt für Probleme entweder (i) eine Lösung oder (ii) eine Abhilfe oder (iii) einen Aktionsplan innerhalb von drei Arbeitstagen nur für Extended-Support-Kunden bereit.
P3	**Mittel:** Ein Vorfall sollte mit der Priorität „mittel" kategorisiert werden, wenn normale Geschäftsprozesse betroffen sind. Das Problem wird durch fehlerhafte Funktionen im Cloud-Service verursacht.	**Erste Reaktion:** Innerhalb von zwei Werktagen nach Einreichung des Falls für osapiens Standard-Support-Kunden oder am nächsten Werktag für Extended-Support-Kunden. **Laufende Kommunikation:** Wenn nicht anders vom osapiens-Support mitgeteilt, einmal alle drei Werktage für Probleme ohne Defekt und zehn Werktage für Probleme mit Produktdefekten.
P4	**Niedrig:** Ein Vorfall sollte mit der Priorität „niedrig" kategorisiert werden, wenn das Problem nur geringe oder keine Auswirkungen auf die normalen Geschäftsprozesse hat. Das Problem wird durch fehlerhafte Funktionen im Cloud-Service verursacht, die nicht täglich benötigt oder selten genutzt werden.	**Erste Reaktion:** Innerhalb von fünf Werktagen nach Einreichung des Falls für Standard-Support-Kunden oder innerhalb von drei Werktagen nach Einreichung des Falls für osapiens Extended-Support-Kunden. **Laufende Kommunikation:** Wenn nicht anders vom osapiens-Support mitgeteilt, einmal pro Woche.

Die folgenden Arten von Vorfällen sind von den oben beschriebenen Reaktionszeiten für den Kunden ausgenommen: (i) Vorfälle, die sich auf ein Release, eine Version bzw. Funktionalitäten der osapiens Cloud Services beziehen, die speziell für den Kunden entwickelt wurden (einschließlich der von osapiens bzw. von osapiens-Tochtergesellschaften entwickelten Services oder einzelner Content-Services); (ii) die dem Vorfall zugrunde liegende Ursache ist keine Fehlfunktion, sondern eine fehlende Funktionalität („Entwicklungsanfrage") oder der Vorfall wird auf eine Beratungsanfrage zurückgeführt („How-to")**;** (iii) der Kunde antwortet nicht innerhalb der oben genannten ersten Reaktionszeiten auf Supportanfragen von osapiens.

AUSGESCHLOSSENE AUSFALLZEIT

Die folgenden Ereignisse sind von der SLA-Systemverfügbarkeitsberechnung ausgeschlossen.

- Geplante Ausfallzeiten und Ereignisse höherer Gewalt.

- Ausfallzeiten von Softwarediensten, wenn die Ursache für die Ausfallzeit außerhalb des Verantwortungsbereichs von osapiens liegt, wie im nächsten Abschnitt dargelegt. Speziell, aber nicht beschränkt auf Vor-Ort-Betriebsmodelle. Zum Beispiel (nicht abschließend):
    - An der Lösung wird vor Ort im eigenen Rechenzentrum des Kunden gearbeitet. Der Cloud-Service ist aufgrund eines Festplattenfehlers nicht verfügbar und es wurde keine Redundanz eingerichtet.
    - An einer Lösung wird vom Kunden vor Ort innerhalb einer virtuellen Umgebung der Cloud-Plattform (z. B. AWS oder Azure) gearbeitet. Der Cloud-Service ist aufgrund von Problemen mit der Netzwerkkonnektivität zwischen der Cloud-Plattform und dem Netzwerk des Kunden nicht verfügbar.

- Ausfallzeiten aufgrund von Unterbrechungen, die durch den Kunden verursacht werden

- Ausfallzeiten aufgrund von Softwarefehlern innerhalb der IT-Landschaft des Kunden oder bei Anwendungen des Kunden, wenn osapiens für die fehlerhafte Komponente nicht verantwortlich ist.

- Ausfallzeiten, die durch Fehler im Netzwerk (einschließlich Internet) oder in Netzwerkkomponenten verursacht werden, wenn der gestörte Bereich des Netzwerks nicht im Verantwortungsbereich von osapiens liegt.
    - Für den Betrieb der Public Cloud Platform sind die Internet-Hubs des osapiens-Rechenzentrums die entsprechenden Übergabestellen, sowohl für Backend- als auch für mobile Client-Verbindungen.
    - Bei anderen Betriebsmodellen wird dies von Fall zu Fall festgelegt, abhängig von den jeweiligen technischen Gegebenheiten.

Verantwortungsmatrix

	Cloud-Service Öffentlich	**Cloud-Service Privat**	**Vor Ort**
SLA-Optionen	Standard oder Extended	Standard oder Extended	Standard oder Extended
Technische Systemüberwachung	osapiens	osapiens	Kunde**
System-Skalierung	osapiens	osapiens	Kunde**
Disaster Failover	osapiens	osapiens	Kunde**
Anwendungs-Updates	osapiens	osapiens	Kunde**
Betriebssystem- und Software-Updates von Drittanbietern	osapiens	osapiens	Kunde**
Wartung der Hardware	osapiens	osapiens	Kunde**

Netzwerk	osapiens*	osapiens*	Kunde**

* Ausgehend von osapiens Service Load Balancer und darüber hinaus. Nicht abgedeckt ist das Netzwerk bzw. die Konnektivität von Systemen und Geräten des osapiens Service Load Balancer (z. B. Internetverbindung).

** Der Kunde selbst oder ein vom Kunden beauftragter Drittparteien-Dienstleister. Die Verantwortung liegt bei osapiens, wenn osapiens selbst vom Kunden für den konkreten Aufgabenbereich beauftragt wurde.

Verantwortlichkeiten des Kunden

11..1 Kundenkontakt. Um einen Support zu erhalten, muss der Kunde mindestens zwei und bis zu fünf qualifizierte englischsprachige Kontaktpersonen (jeweils ein „Customer Contact", „Designated Support Contact", „Authorized Support Contact", „Key User" oder „Application Administrator" - Rollen von Systemadministratoren innerhalb bestimmter Cloud-Services) benennen, die berechtigt sind, den osapiens-Support zu kontaktieren oder darauf zuzugreifen. Der Kundenkontakt ist verantwortlich für die Verwaltung aller geschäftsbezogenen Aufgaben des Cloud-Service im Zusammenhang mit dem Geschäft des Kunden, wie z. B.:

(i) Unterstützung des Endanwenders und Verwaltung seiner Vorfälle. Dazu gehört die Suche nach bekannten Lösungen in der verfügbaren Dokumentation und die Kontaktaufnahme mit dem osapiens-Support bei neuen Problemen;

(ii) Verwaltung von Hintergrundjobs und Aufteilung von Geschäftsaufgaben auf Benutzer (falls vorhanden);

(iii) Verwaltung und Überwachung von Verbindungen zu Fremdsystemen des Kunden (falls vorhanden);

(iv) (iv) Unterstützung bei der Einführung des Cloud-Service.

11.2 Kontaktdaten. Der Kunde muss Kontaktdaten (insbesondere E-Mail-Adresse und Telefonnummer) angeben, unter denen der Kundenkontakt oder der Bevollmächtigte des Kundenkontakts jederzeit erreichbar ist. Der Kunde muss seine Kundenkontakte für einen Cloud-Service über das osapiens-Supportportal unter https://support.osapiens.comaktualisieren.Nur autorisierte Kundenkontakte dürfen die Supportorganisation von osapiens kontaktieren.

11.3 Zusammenarbeit. Um Supportleistungen zu erhalten und um Supportvorfälle zu lösen, muss der Kunde in angemessener Weise mit osapiens zusammenarbeiten und er muss über ausreichendes technisches Fachwissen und Kenntnisse über seine Konfiguration des Cloud-Service verfügen, um osapiens relevante Informationen zur Verfügung zu stellen, die es ermöglichen, den aufgetretenen Fehler festzustellen und zu beheben, wie z. B. Referenz-ID, Problembeispiele, Bildschirmfotos.

11.4 Zusammenarbeit Auf Verlangen des Kunden muss osapiens den Kunden bei der Analyse des Vorfalls angemessen unterstützen, auch wenn ein Vorfall im Zusammenhang mit anderen Leistungen des Kunden oder anderer Dritter auftritt. osapiens muss seine Fehleranalyse zur Verfügung stellen und mit dem Kunden sowie beauftragten Dritten bei der Analyse und Beseitigung von Vorfällen angemessen zusammenarbeiten, soweit dies zumutbar ist. Ist osapiens für den Vorfall nicht verantwortlich, muss der Kunde den durch diese Klausel verursachten zeitlichen und materiellen Aufwand mit einem einvernehmlich festgelegten Stundensatz vergüten.

VEREINBARUNG ZUR VERARBEITUNG PERSONENBEZOGENER DATEN FÜR osapiens CLOUD-SERVICES

1. HINTERGRUND

1.1 Zweck und Anwendungsbereich. Dieses Dokument („**DPA**") ist Bestandteil der Vereinbarung und bildet einen Teil eines schriftlichen (auch in elektronischer Form) Vertrags zwischen osapiens und dem Kunden. Diese DPA gilt für personenbezogene Daten, die von osapiens und seinen Unterauftragsverarbeitern im Zusammenhang mit der Bereitstellung des Cloud-Service verarbeitet werden. Diese DPA gilt nicht außerhalb der Produktionsumgebungen des Cloud-Service, wenn solche Umgebungen von osapiens zur Verfügung gestellt werden, und der Kunde darf in solchen Umgebungen keine personenbezogenen Daten speichern.

1.3 DSGVO. osapiens und der Kunde vereinbaren, dass es in der Verantwortung jeder Partei liegt, die Anforderungen zu überprüfen und zu übernehmen, die den Verantwortlichen und Verarbeitern durch die Datenschutz-Grundverordnung 2016/679 („**DSGVO**") auferlegt werden, insbesondere im Hinblick auf die Artikel 28 und 32 bis 36 der GDPR, wenn und soweit sie auf personenbezogene Daten des Kunden/Verantwortlichen anwendbar sind, die im Rahmen der DPA verarbeitet werden.

1.4 Governance. osapiens agiert als Auftragsverarbeiter und Kunde, wobei die Unternehmen, denen er die Nutzung des Cloud-Service gestattet, als Verantwortliche im Sinne der DPA agieren. Der Kunde fungiert als einziger Ansprechpartner und ist allein verantwortlich für die Einholung aller relevanten Genehmigungen, Zustimmungen und Erlaubnisse für die Verarbeitung personenbezogener Daten gemäß dieser DSGVO, einschließlich, falls zutreffend, der Zustimmung der Controller zur Nutzung von osapiens als Auftragsverarbeiter. Werden vom Kunden Genehmigungen, Zustimmungen, Anweisungen oder Erlaubnisse erteilt, so erfolgen diese nicht nur im Namen des Kunden, sondern auch im Namen aller anderen Controller, die den Cloud-Service nutzen. Wenn osapiens den Kunden informiert oder benachrichtigt, gilt diese Information oder Benachrichtigung als bei denjenigen Controllern eingegangen, denen der Kunde die Nutzung des Cloud-Service gestattet hat, und es liegt in der Verantwortung des Kunden, diese Informationen und Benachrichtigungen an die entsprechenden Controller weiterzuleiten.

2. VERPFLICHTUNGEN von osapiens

2.1 Weisungen des Kunden. osapiens darf personenbezogene Daten nur gemäß den dokumentierten Weisungen des Kunden verarbeiten. Der Vertrag (einschließlich dieser DPA) stellt eine solche dokumentierte Erstanweisung dar, und jede Nutzung des Cloud-Service bildet dann eine weitere Anweisung. osapiens muss sich im Rahmen des Zumutbaren bemühen, etwaige weitere Anweisungen des Kunden zu befolgen, sofern sie datenschutzrechtlich erforderlich und technisch möglich sind und keine Änderungen des Cloud-Service erfordern. Wenn eine der vorgenannten Ausnahmen zutrifft oder osapiens aus anderen Gründen

eine Weisung nicht einhalten kann oder der Meinung ist, dass eine Weisung gegen das Datenschutzrecht verstößt, muss osapiens den Kunden unverzüglich darüber informieren (E-Mail zulässig).

3.2 Verarbeitung auf gesetzlicher Grundlage. osapiens kann personenbezogene Daten auch verarbeiten, wenn dies durch geltendes Recht vorgeschrieben ist. In einem solchen Fall muss osapiens den Kunden vor der Verarbeitung über diese gesetzliche Verpflichtung informieren, es sei denn, das Gesetz verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses.

3.3 Personal. Zur Verarbeitung personenbezogener Daten dürfen osapiens und seine Unterauftragsverarbeiter nur autorisiertem Personal, das sich zur Vertraulichkeit verpflichtet hat, Zugang gewähren. osapiens und seine Unterauftragsverarbeiter müssen das Personal, das Zugang

zu personenbezogenen Daten hat, regelmäßig in den geltenden Datensicherheits- und Datenschutzmaßnahmen schulen.

3.4 Zusammenarbeit. Auf Wunsch des Kunden muss osapiens in angemessener Weise mit dem Kunden und den Controllern zusammenarbeiten, wenn es um Anfragen von betroffenen Personen oder Aufsichtsbehörden bezüglich der Verarbeitung personenbezogener Daten durch osapiens oder eines Verstoßes gegen das Datenschutzgesetz geht. osapiens muss den Kunden so schnell wie möglich über jede Anfrage informieren, die es von einer betroffenen Person in Bezug auf die Verarbeitung personenbezogener Daten erhalten hat, ohne selbst auf eine solche Anfrage ohne weitere Anweisungen des Kunden zu reagieren. osapiens muss Funktionen bereitstellen, die den Kunden dabei unterstützen, personenbezogene Daten zu korrigieren oder aus dem Cloud-Service zu entfernen oder ihre Verarbeitung gemäß dem Datenschutzgesetz einzuschränken. Wird eine solche Funktionalität nicht zur Verfügung gestellt, muss osapiens gemäß den Anweisungen des Kunden und den Datenschutzgesetzen die personenbezogenen Daten korrigieren, entfernen oder deren Verarbeitung einschränken.

3.5 Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten. osapiens muss den Kunden unverzüglich benachrichtigen, nachdem es von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat, und die in seinem Besitz befindlichen Informationen in angemessener Weise zur Verfügung stellen, um den Kunden bei der Erfüllung seiner Verpflichtungen zur Meldung einer entsprechenden Verletzung gemäß den Datenschutzgesetzen zu unterstützen. osapiens kann diese Informationen nach und nach zur Verfügung stellen, sobald sie verfügbar sind. Eine solche Benachrichtigung ist nicht als Eingeständnis eines Verschuldens oder einer Haftung von osapiens zu verstehen oder auszulegen.

3.6 Datenschutz-Folgenabschätzung. Wenn der Kunde (oder seine Controller) aufgrund von Datenschutzgesetzen verpflichtet ist, eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation mit einer Aufsichtsbehörde durchzuführen, muss osapiens auf Anfrage des Kunden solche Dokumente zur Verfügung stellen, die allgemein für den Cloud-Service verfügbar sind (z. B. diese DPA, den Vertrag, Prüfberichte oder Zertifizierungen). Jede zusätzliche Unterstützung muss von den Parteien einvernehmlich vereinbart werden.

4. DATENEXPORT UND -LÖSCHUNG

4.1 Export und Abruf durch den Kunden. Während der Laufzeit des Abonnements und vorbehaltlich der Vereinbarung kann der Kunde jederzeit auf seine persönlichen Daten zugreifen. Der Kunde kann seine persönlichen Daten in einem Standardformat exportieren und abrufen. Der Export und Abruf kann technischen Beschränkungen unterliegen. In diesem Fall müssen osapiens und der Kunde eine angemessene Methode finden, um dem Kunden den Zugriff auf die personenbezogenen Daten zu ermöglichen.

4.2 Löschung. Vor Ablauf der Abonnementlaufzeit kann der Kunde die Self-Service-Export-Tools von osapiens (soweit verfügbar) nutzen, um einen endgültigen Export der personenbezogenen Daten aus dem Cloud-Service durchzuführen (was eine „Rückgabe" der personenbezogenen Daten darstellt). Am Ende der Laufzeit des Abonnements weist der Kunde osapiens an, die auf den Servern, auf denen der Cloud-Service gehostet wird, verbleibenden personenbezogenen Daten innerhalb eines angemessenen Zeitraums (max. sechs Monate) gemäß dem Datenschutzrecht zu löschen, es sei denn, das geltende Recht schreibt eine Aufbewahrung vor.

5. Prüfrechte

5.1 Prüfrechte. Vorbehaltlich dieser Abschnitts 5 muss osapiens dem Kunden auf Anfrage alle Informationen zur Verfügung stellen, die für den Nachweis der Einhaltung dieses Vertrags erforderlich sind, und ermöglicht Prüfungen, einschließlich Inspektionen, durch den Kunden oder einen vom Kunden beauftragten Prüfer in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden durch osapiens und arbeitet daran mit.

5.2 Beschränkung. Auskunfts- und Prüfrechte des Kunden ergeben sich aus Abschnitt 5.1 nur insoweit, als der Vertrag ihm nicht anderweitig Auskunfts- und Prüfrechte einräumt, die den einschlägigen datenschutzrechtlichen Anforderungen genügen.

5.2 Prüfumfang. Der Kunde muss jede Prüfung mindestens sechzig Tage im Voraus ankündigen, es sei denn, zwingende Datenschutzgesetze oder eine zuständige Datenschutzbehörde verlangen eine kürzere Ankündigung. Häufigkeit und Umfang der Prüfungen werden von den Parteien nach Treu und Glauben einvernehmlich festgelegt. Kunden-Prüfungen sind zeitlich auf maximal drei Arbeitstage begrenzt. Über solche Einschränkungen hinaus müssen die Parteien aktuelle Zertifizierungen oder andere Prüfberichte verwenden, um wiederholte Prüfungen zu vermeiden oder zu minimieren. Der Kunde muss osapiens die Ergebnisse einer Prüfung zur Verfügung stellen.

5.3 Kosten für Prüfungen. Der Kunde trägt die Kosten einer Prüfung, es sei denn, die Prüfung ergibt einen wesentlichen Verstoß von osapiens gegen diese DPA, dann trägt osapiens seine eigenen Kosten einer Prüfung. Sollte bei einer Prüfung festgestellt werden, dass osapiens gegen seine Verpflichtungen aus der DPA verstoßen hat, muss osapiens den Verstoß unverzüglich auf eigene Kosten beheben.

6. UNTERAUFTRAGSVERARBEITER

6.1 Erlaubte Nutzung. osapiens erhält eine generelle Erlaubnis, die Verarbeitung personenbezogener Daten an Unterauftragsverarbeiter zu vergeben, vorausgesetzt, dass:

(a) osapiens Unterauftragsverarbeiter im Rahmen eines schriftlichen Vertrags (auch in elektronischer Form) beauftragt, der mit den Bedingungen dieser DPA in Bezug auf die Verarbeitung personenbezogener Daten durch den Unterauftragsverarbeiter übereinstimmt. osapiens haftet für Verstöße des Unterauftragsverarbeiters gemäß den Bedingungen dieser Vereinbarung.

(b) osapiens muss die Sicherheits-, Datenschutz- und Vertraulichkeitspraktiken eines Unterauftragsverarbeiters vor der Auswahl bewerten, um festzustellen, ob dieser in der Lage ist, das in dieser DPA geforderte Schutzniveau für personenbezogene Daten zu gewährleisten; und

7. INTERNATIONALE VERARBEITUNG

7.1 Bedingungen für die internationale Verarbeitung. osapiens ist berechtigt, personenbezogene Daten, auch unter Verwendung von Unterauftragsverarbeitern, nach Maßgabe dieser DPA außerhalb des Landes zu verarbeiten, in dem der Kunde seinen Sitz hat, soweit dies datenschutzrechtlich zulässig ist.

7.2 Standardvertragsklauseln. Wenn (i) personenbezogene Daten eines im EWR oder in der Schweiz ansässigen Controllers in einem Land außerhalb des EWR, der Schweiz und eines Landes, einer Organisation oder eines Gebiets verarbeitet werden, das von der Europäischen Union als sicheres Land mit einem angemessenen Datenschutzniveau gemäß Art. 45 DSGVO anerkannt ist, oder wenn (ii) personenbezogene Daten eines anderen Controllers international verarbeitet werden und diese internationale Verarbeitung eine Angemessenheitsregelung nach dem Recht des Landes des Controllers erfordert und die erforderliche Angemessenheitsregelung durch den Abschluss von Standardvertragsklauseln erfüllt werden kann,

(a) können osapiens und der Kunde die Standardvertragsklauseln vereinbaren.

(b) Der Kunde schließt die Standardvertragsklauseln mit jedem relevanten Unterauftragsverarbeiter wie folgt ab, entweder (i) der Kunde tritt den von osapiens und dem Unterauftragsverarbeiter abgeschlossenen Standardvertragsklauseln als eigenständiger Inhaber von Rechten und Pflichten bei („Beitrittsmodell") oder (ii) der Unterauftragsverarbeiter (vertreten durch osapiens) schließt die Standardvertragsklauseln mit dem Kunden ab („Vollmachtsmodell"). Das Vollmachtsmodell kommt zur Anwendung, wenn und soweit osapiens ausdrücklich bestätigt hat, dass ein Unterauftragsverarbeiter dafür in Frage kommt, und zwar über die unter Abschnitt 6.1(c) bereitgestellte Unterauftragsverarbeiterliste oder eine Mitteilung an den Kunden; oder

(c) andere Verantwortliche, deren Nutzung der Cloud-Services vom Kunden im Rahmen der Vereinbarung genehmigt wurde, können ebenfalls Standardvertragsklauseln mit osapiens bzw. den entsprechenden Unterauftragsverarbeitern in der gleichen Weise wie der Kunde gemäß den vorstehenden Abschnitten 7.2 (a) und (b) abschließen. In diesem Fall muss der Kunde die Standardvertragsklauseln im Namen der anderen Controller abschließen.

7.3 Bezug der Standardvertragsklauseln zum Vertrag. Nichts in der Vereinbarung ist so auszulegen, dass es Vorrang vor einer widersprüchlichen Klausel der Standardvertragsklauseln hat. Zur Klarstellung: Wo diese DPA in den Abschnitten 5 und 6 Regeln für Prüfungen und Unterauftragsverarbeiter weiter spezifiziert, gelten diese Spezifikationen auch in Bezug auf die Standardvertragsklauseln.

7.4 Anwendbares Recht der Standardvertragsklauseln. Die Standardvertragsklauseln unterliegen dem Recht des Landes, in dem der jeweilige Controller seinen Sitz hat.

8. DOKUMENTATION; AUFZEICHNUNGEN ÜBER DIE VERARBEITUNG

Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für das Führen von Aufzeichnungen über die Verarbeitung, soweit dies datenschutzrechtlich erforderlich ist. Jede Partei muss die andere Partei in angemessener Weise bei der Erfüllung ihrer Dokumentationspflichten, einschließlich der Bereitstellung der von der anderen Partei benötigten Informationen in einer von der anderen Partei in angemessener Weise geforderten Weise (z. B. unter Verwendung eines elektronischen Systems) unterstützen, um die andere Partei in die Lage zu versetzen, etwaige Verpflichtungen in Bezug auf die Führung von Aufzeichnungen über die Verarbeitung zu erfüllen.

9. EU-ZUGANG

9.1 Optionaler Service. Der EU-Zugang ist ein optionaler Service, der von osapiens angeboten werden kann. osapiens stellt den für den EU-Zugang in Frage kommenden Cloud-Service nach Maßgabe dieses Abschnitts 9 bereit. Wenn der EU-Zugang nicht ausdrücklich im Bestellformular angegeben und vereinbart ist, gilt dieser Abschnitt 9 nicht.

9.2 EU-Zugang. osapiens darf nur europäische Unterauftragsverarbeiter einsetzen, um Support in Bezug auf den Zugang zu den personenbezogenen Daten im Cloud-Service zu leisten und osapiens darf keine personenbezogenen Daten außerhalb des EWR oder der Schweiz exportieren, es sei denn, der Kunde hat dies von Fall zu Fall ausdrücklich schriftlich (auch per E-Mail genehmigt); oder wie in Abschnitt 9.4 ausgeschlossen.

9.3 Standort des Rechenzentrums. Zum Zeitpunkt des Inkrafttretens der Vereinbarung befinden sich die Rechenzentren, die zum Hosten der personenbezogenen Daten im Cloud-Service verwendet werden, im EWR oder in der Schweiz. osapiens darf die Instanz des Kunden nicht ohne vorherige schriftliche Zustimmung des Kunden (auch per E-Mail) in ein Rechenzentrum außerhalb des EWR oder der Schweiz migrieren. Wenn osapiens plant, die Instanz des Kunden in ein Rechenzentrum innerhalb des EWR oder in die Schweiz zu migrieren, muss osapiens den Kunden spätestens dreißig Tage vor der geplanten Migration schriftlich (auch per E-Mail) informieren.

9.4 Ausschlüsse. Die folgenden personenbezogenen Daten unterliegen nicht den Abschnitten 9.2 und 9.3:

(a) Kontaktdaten des Absenders eines Support-Tickets; und

(b) alle anderen personenbezogenen Daten, die der Kunde beim Einreichen eines Support-Tickets übermittelt. Der Kunde kann sich dafür entscheiden, keine personenbezogenen Daten zu übermitteln, wenn er ein Support-Ticket einreicht.

10. BEGRIFFSBESTIMMUNGEN

Großgeschriebene Begriffe, die hier nicht definiert sind, haben die Bedeutungen aus der Vereinbarung.

10.1 „Controller" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von

personenbezogenen Daten entscheidet; für die Zwecke dieser DPA gilt der Kunde, wenn er als Auftragsverarbeiter für einen anderen Verantwortlichen handelt, in Bezug auf osapiens als zusätzlicher und unabhängiger Controller mit den entsprechenden Rechten und Pflichten gemäß dieser DPA.

10.2 „Rechenzentrum" bezeichnet den Standort, an dem die Produktionsinstanz des Cloud-Service für den Kunden gehostet wird.

10.3 „Datenschutzgesetz" bezeichnet die geltende Gesetzgebung zum Schutz der Grundrechte und -freiheiten von Personen und ihres Rechts auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten im Rahmen der Vereinbarung (und umfasst, soweit es die Beziehung zwischen den Parteien in Bezug auf die Verarbeitung personenbezogener Daten durch osapiens im Auftrag des Kunden betrifft, die DSGVO als Mindeststandard, unabhängig davon, ob die personenbezogenen Daten der DSGVO unterliegen oder nicht).

10.4 „Betroffene Person" ist eine identifizierte oder identifizierbare natürliche Person im Sinne des Datenschutzgesetzes.

10.5 „EWR" bezeichnet den Europäischen Wirtschaftsraum, also die Mitgliedstaaten der Europäischen Union sowie Island, Liechtenstein und Norwegen.

10.6 „Europäischer Unterauftragsverarbeiter" bezeichnet einen Unterauftragsverarbeiter, der physisch personenbezogene Daten im EWR oder in der Schweiz verarbeitet.

10.7 „Personenbezogene Daten" sind alle Informationen über eine betroffene Person, die durch das Datenschutzgesetz geschützt sind. Für die Zwecke der DPA umfassen sie nur personenbezogene Daten, die (i) vom Kunden oder seinen autorisierten Nutzern in den Cloud-Service eingegeben oder aus dessen Nutzung abgeleitet werden,

oder (ii) die osapiens oder seinen Unterauftragsverarbeitern zur Verfügung gestellt werden oder auf die sie zugreifen, um Unterstützung im Rahmen der Vereinbarung zu leisten. Personenbezogene Daten sind eine Teilmenge der Kundendaten (wie in der Vereinbarung definiert).

10.8 „Verletzung des Schutzes personenbezogener Daten" bezeichnet eine bestätigte (1) versehentliche oder unrechtmäßige Zerstörung, einen Verlust, eine Änderung, eine unbefugte Offenlegung oder einen unbefugten Zugriff Dritter auf personenbezogene Daten oder (2) einen ähnlichen Vorfall, der personenbezogene Daten betrifft, in Bezug auf den ein Controller nach dem Datenschutzgesetz verpflichtet ist, die zuständigen Datenschutzbehörden oder die betroffenen Personen zu benachrichtigen.

10.9 „Auftragsverarbeiter" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Controllers verarbeitet, sei es direkt als Auftragsverarbeiter eines Controllers oder indirekt als Unterauftragsverarbeiter eines Auftragsverarbeiters, der personenbezogene Daten im Auftrag des Controllers verarbeitet.

10.10 „Standardvertragsklauseln" oder manchmal auch „EU-Musterklauseln" bezeichnen die (Standardvertragsklauseln [Auftragsverarbeiter]) oder jede spätere Version davon, die von der Europäischen Kommission veröffentlicht wird (und die automatisch gilt).

10.11 „Unterauftragsverarbeiter" bezeichnet die verbundenen Unternehmen von osapiens und Dritte, die von osapiens und den verbundenen Unternehmen von osapiens in Verbindung mit dem Cloud-Service beauftragt werden und die personenbezogene Daten gemäß dieser DPA verarbeiten.

osapiens

Anhang 1 zur DPA

Standardvertragsklauseln (Verarbeiter)[1]

Für die Zwecke von Artikel 26, Absatz 2 der Richtlinie 95/46/EG (bzw. nach dem 25. Mai 2018, Artikel 44 ff. der Verordnung 2016/79) für die Übermittlung personenbezogener Daten an Verarbeiter mit Sitz in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten

[...]

(in den Klauseln im Folgenden als „**Datenexporteur"** bezeichnet)

und

[...]

(in den Klauseln im Folgenden als „**Datenimporteur"** bezeichnet)

einzeln eine „Partei"; zusammen „die Parteien",

SIND über die folgenden Vertragsklauseln (die Klauseln) ÜBEREINGEKOMMEN, um angemessene Garantien in Bezug auf den Schutz der Privatsphäre und der Grundrechte und -freiheiten natürlicher Personen für die Übermittlung der in Anhang 1 aufgeführten personenbezogenen Daten durch den Datenexporteur an den Datenimporteur zu schaffen.

Klausel 1

Begriffsbestimmungen

Für die Zwecke der Klauseln:

(a) „Personenbezogene Daten", „besondere Kategorien von Daten", „Verarbeitung", „Controller", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" haben die gleiche Bedeutung wie in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr([1]);

(b) der „Datenexporteur" ist der Controller, der die personenbezogenen Daten übermittelt;

(c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten zu erhalten, die nach der Übermittlung gemäß seinen Anweisungen und den Bestimmungen der Klauseln in seinem Namen verarbeitet werden sollen, und der nicht dem System eines Drittlandes unterliegt, das einen angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

(d) der „Unterauftragsverarbeiter" ist jeder vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs beauftragte Auftragsverarbeiter, der sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten zu erhalten, die ausschließlich für Verarbeitungstätigkeiten bestimmt sind, die nach der Übermittlung im Auftrag des Datenexporteurs gemäß seinen Anweisungen, den Bestimmungen der Klauseln und den Bestimmungen des schriftlichen Untervertrags durchgeführt werden sollen;

[1] Gemäß dem Beschluss der Kommission vom 5. Februar 2010 (2010/87/EU)

(e) das „geltende Datenschutzrecht" bezeichnet die Rechtsvorschriften zum Schutz der Grundrechte und -freiheiten natürlicher Personen und insbesondere ihres Rechts auf Privatsphäre in Bezug auf die

---

Verarbeitung personenbezogener Daten, die für einen Controller in dem Mitgliedstaat gelten, in dem der Datenexporteur niedergelassen ist;

(f) „technische und organisatorische Sicherheitsmaßnahmen" sind Maßnahmen zum Schutz personenbezogener Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust, unberechtigte Änderung, unberechtigte Weitergabe oder gegen unberechtigten Zugang (insbesondere wenn die Verarbeitung die Übermittlung von Daten über ein Netzwerk umfasst) und gegen jede andere Form der unrechtmäßigen Verarbeitung.

Klausel 2

Details zur Übertragung

Die Einzelheiten der Übertragung und insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, sind in Anhang 1 aufgeführt, der wesentlicher Bestandteil der Klauseln ist.

Klausel 3

Klausel zu Drittbegünstigten

1. Die betroffene Person kann diese Klausel, Klausel 4 (b) bis (i), Klausel 5 (a) bis (e) und (g) bis (j), Klausel 6 (1) und (2), Klausel 7, Klausel 8 (2) und die Klauseln 9 bis 12 als Drittbegünstigter gegenüber dem Datenexporteur geltend machen.

2. Die betroffene Person kann diese Klausel, Klausel 5 (a) bis (e) und (g), die Klauseln 6 und 7, Klausel 8 (2) sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn der Datenexporteur faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

3. Die betroffene Person kann diese Klausel, Klausel 5 (a) bis (e) und (g), die Klauseln 6 und 7, Klausel 8 (2) sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl der Datenexporteur als auch der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen eigene Verarbeitungstätigkeiten gemäß den Klauseln beschränkt.

4. Die Parteien erheben keine Einwände dagegen, dass eine betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

osapiens

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich damit einverstanden und garantiert:

(a) dass die Verarbeitung der personenbezogenen Daten einschließlich der Übertragung gemäß den maßgeblichen Bestimmungen der geltenden Datenschutzgesetze durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaates mitgeteilt wurde, in dem der Datenexporteur ansässig ist) und nicht gegen die maßgeblichen Bestimmungen dieses Staates verstößt;

(b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übertragenen personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit den geltenden Datenschutzgesetzen und den Klauseln zu verarbeiten;

(c) dass der Datenimporteur hinreichende Garantien in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsvorkehrungen bietet;

(d) dass die Sicherheitsvorkehrungen nach einer Einschätzung der Anforderungen der geltenden Datenschutzgesetze hinreichend gewährleisten, dass personenbezogene Daten vor unbeabsichtigter oder rechtswidriger Zerstörung oder unbeabsichtigtem Verlust, unbeabsichtigter Änderung, unbefugter Offenlegung oder unbefugtem Zugriff, insbesondere, wenn die Daten im Rahmen ihrer Verarbeitung über ein Netzwerk übertragen werden, sowie vor allen anderen rechtswidrigen Formen der Verarbeitung geschützt sind und dass diese Vorkehrungen ein ausreichendes Sicherheitsniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten im Hinblick auf den Stand der Technik und die bei ihrer Umsetzung entstehenden Kosten gerecht wird;

(e) dass er für die Einhaltung dieser Sicherheitsvorkehrungen sorgt;

(f) dass die betroffene Person, sofern die Übertragung besondere Datenkategorien beinhaltet, vor oder so bald wie möglich nach der Übertragung davon in Kenntnis gesetzt wurde oder wird, dass seine Daten in ein Drittland übertragen werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

(g) er die gemäß Klausel 5 (b) sowie Klausel 8 (3) vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Datenschutz-Aufsichtsbehörde weiterleitet, wenn der Datenexporteur beschließt, die Übertragung fortzusetzen oder die Aussetzung aufzuheben;

(h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsvorkehrungen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls eine Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

(i) bei einer Unterauftragsverarbeitung diese gemäß Klausel 11 durch einen Unterauftragsverarbeiter erfolgt, der die personenbezogenen Daten und die Rechte der

betroffenen Personen mindestens ebenso schützt, wie dies vom Datenimporteur nach diesen Klauseln verlangt wird; und

(j) dass er die Einhaltung der Klausel 4 (a) bis (i) gewährleistet.

Klausel 5

Pflichten des Datenimporteurs ([2])

Der Datenimporteur erklärt sich damit einverstanden und garantiert:

(a) dass er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und gemäß dessen Anweisungen und den Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübertragung auszusetzen bzw. den Vertrag zu kündigen;

(b) dass er seines Wissens keinen Gesetzen unterliegt, die ihn an der Befolgung der Anweisungen des Datenexporteurs und der Einhaltung seiner vertraglichen Pflichten hindern, und dass er eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die durch die Klauseln gebotenen Garantien und Pflichten auswirkt, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erlangt; in diesem Fall ist der Datenexporteur berechtigt, die Datenübertragung auszusetzen bzw. den Vertrag zu kündigen;

(c) dass er vor der Verarbeitung der übertragenen personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsvorkehrungen ergriffen hat;

(d) dass er den Datenexporteur unverzüglich informiert über:

(i) alle rechtsverbindlichen Aufforderungen einer Strafverfolgungsbehörde zur Offenlegung der personenbezogenen Daten, sofern dem nicht ein Verbot entgegensteht, z. B. ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses in einer Strafsache;

(ii) jeden unbeabsichtigten oder unbefugten Zugriff; und

(iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

(e) dass er alle Anfragen des Datenexporteurs bezüglich seiner Verarbeitung der übertragenen personenbezogenen Daten unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Aufsichtsbehörde im Hinblick auf die Verarbeitung der übertragenen Daten befolgt;

(f) dass er auf Verlangen des Datenexporteurs seine Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einer vom Datenexporteur ggf. in Absprache mit der Aufsichtsbehörde ausgewählten Prüfstelle, deren Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind, durchgeführt werden;

(g) dass er den betroffenen Personen auf Anfrage eine Kopie der Klauseln oder eines bestehenden Vertrags über die Unterauftragsverarbeitung zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden, mit Ausnahme von Anhang 2; dieser wird durch eine allgemeine Beschreibung der Sicherheitsvorkehrungen ersetzt, wenn die betroffenen Personen vom Datenexporteur keine Kopie erhalten können;

(h) dass er im Fall einer Unterauftragsverarbeitung den Datenexporteur zuvor benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

(i) dass der Unterauftragsverarbeiter die Datenverarbeitungsdienste gemäß Klausel 11 erbringt;

(j) dass er dem Datenexporteur unverzüglich eine Kopie jedes Vertrags über einen Unterverarbeitungsauftrag zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

1. Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

2. Wenn eine betroffene Person nicht in der Lage ist, Schadenersatzansprüche gemäß Absatz 1 gegenüber dem Datenexporteur wegen eines Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen die in den Klauseln 3 oder 11 genannten Pflichten geltend zu machen, weil der Datenexporteur faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person ihre Ansprüche ihm gegenüber anstelle des Datenexporteurs geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber diesem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß gegen seine Verpflichtungen beruft.

3. Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen die in den Klauseln 3 und 11 aufgeführten Pflichten Ansprüche geltend zu machen, weil sowohl der Datenexporteur als auch der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm anstatt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Die Haftung des Unterauftragsverarbeiters ist auf dessen eigene Datenverarbeitungstätigkeiten nach diesen Klauseln beschränkt.

osapiens

Klausel 7

Schlichtungsverfahren und Gerichtsbarkeit

1. Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigter bzw. Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

(a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Aufsichtsbehörde beizulegen oder

(b) den Streitfall den Gerichten des Mitgliedstaates, in dem der Datenexporteur ansässig ist, vorzulegen.

2. Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Aufsichtsbehörden

1. Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

2. Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

3. Der Datenimporteur muss den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis setzen, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 (b) vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Geltendes Recht

Diese Klauseln unterliegen dem Recht des Mitgliedstaates, in dem der Datenexporteur ansässig ist.

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, bei Bedarf weitere geschäftsbezogene Klauseln aufzunehmen, solange diese nicht im Widerspruch zu der Klausel stehen.

osapiens

Klausel 11

Unterauftragsverarbeitung

1. Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur durch eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss (3). Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

2. Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6, Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen eigene Verarbeitungstätigkeiten nach den Klauseln beschränkt.

3. Für Datenschutzbestimmungen im Zusammenhang mit der Unterauftragsverarbeitung des Vertrags gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur ansässig ist.

4. Der Datenexporteur muss ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen führen, die vom Datenimporteur nach Klausel 5 (j) übermittelt wurden. Das Verzeichnis muss der Aufsichtsbehörde des Datenexporteurs zur Verfügung stehen.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

1. Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Erbringung von Datenverarbeitungsdienstleistungen nach Wahl des Datenexporteurs alle übermittelten personenbezogenen Daten und die Kopien davon an den Datenexporteur zurückgeben oder alle personenbezogenen Daten vernichten und dies dem Datenexporteur gegenüber bescheinigen muss, es sei denn, der Datenimporteur ist aufgrund gesetzlicher Vorschriften daran gehindert, alle oder einen Teil der übermittelten personenbezogenen Daten zurückzugeben oder zu vernichten. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übertragenen personenbezogenen Daten gewährleistet und diese übertragenen persönlichen Daten nicht mehr aktiv weiterverarbeitet.

2. Der Datenimporteur und der Unterauftragsverarbeiter gewährleisten, dass sie auf Verlangen des Datenexporteurs bzw. der Aufsichtsbehörde ihre Datenverarbeitungseinrichtungen für eine Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen werden.

(1) Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

(2) Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 (1) der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

(3) Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mit unterzeichnet.

osapiens

ANHANG 1 ZU DEN STANDARDVERTRAGSKLAUSELN

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Datenexporteur

Der Datenexporteur ist in diesen Modellklauseln als die **datenexportierende Organisation** definiert.

Datenimporteur

osapiens und seine Unterauftragnehmer stellen den Cloud-Service zur Verfügung, der den folgenden Support beinhaltet:
osapiens unterstützt die Cloud-Service-Rechenzentren aus der Ferne von osapiens Einrichtungen aus, in denen osapiens Personal beschäftigt. Die Unterstützung umfasst:

- *Überwachung des Cloud-Service*
- *Sicherung & Wiederherstellung der im Cloud-Service gespeicherten Kundendaten*
- *Freigabe und Entwicklung von Fixes und Upgrades für den Cloud-Service*
- *Überwachung, Fehlerbehebung und Verwaltung der zugrunde liegenden Cloud-Service-Infrastruktur und Datenbank*
- *Sicherheitsüberwachung, Unterstützung bei netzwerkbasierter Eindringungserkennung, Penetrationstests*

osapiens leistet Support, wenn ein Kunde ein Support-Ticket einreicht, weil der Cloud-Service für einige oder alle autorisierten Nutzer nicht verfügbar ist oder nicht wie erwartet funktioniert. osapiens nimmt Anrufe entgegen und führt grundlegende Fehlerbehebungen durch und bearbeitet Support-Tickets in einem Tracking-System, das von der Produktionsinstanz des Cloud-Service getrennt ist.

Betroffene Personen

Die übermittelten personenbezogenen Daten beziehen sich auf folgende Kategorien betroffener Personen:

Sofern vom Datenexporteur nicht anders angegeben, beziehen sich die übertragenen personenbezogenen Daten auf die folgenden Kategorien betroffener Personen: Mitarbeiter, Auftragnehmer, Geschäftspartner oder andere Personen, deren personenbezogene Daten im Cloud-Service gespeichert sind.

Kategorien von Daten

Die übermittelten personenbezogenen Daten betreffen die folgenden Datenkategorien:

Persönliche Details, einschließlich: Vor- und Nachname; geschäftliche E-Mail- und Telefondaten; Informationen, die Mitarbeiter des Kunden über die Cloud-Services übermitteln, Standortdaten, Gerätedaten, einschließlich der Internetprotokoll (IP)-Adresse, die verwendet wird, um ihre Computer mit dem Internet zu verbinden, ihre Anmeldeinformationen, Browsertyp und -version, Zeitzoneneinstellung, Browser-Plug-in-Typen und -Versionen, Betriebssystem und Plattform.

Besondere Datenkategorien (falls zutreffend)

Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben): *NA*

Verarbeitungsprozesse

Die übermittelten personenbezogenen Daten unterliegen den folgenden grundlegenden Verarbeitungstätigkeiten:

- *Verwendung personenbezogener Daten zum Einrichten, Betreiben, Überwachen und Bereitstellen des Cloud-Service (einschließlich betrieblicher und technischer Unterstützung)*
- *Erbringung von Beratungsleistungen;*
- *Kommunikation mit autorisierten Benutzern*
- *Speicherung von personenbezogenen Daten in dedizierten Rechenzentren (Multi-Tenant-Architektur)*
- *Hochladen aller Korrekturen oder Upgrades auf den Cloud-Service*
- *Sicherung der personenbezogenen Daten*
- *Computerverarbeitung personenbezogener Daten, einschließlich Datenübertragung, Datenabruf und Datenzugriff*
- *Netzwerkzugriff, um die Übertragung personenbezogener Daten zu ermöglichen*
- *Ausführung von Weisungen des Kunden nach Maßgabe der Vereinbarung.*

osapiens

ANHANG 2 ZU DEN STANDARDVERTRAGSKLAUSELN

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 (d) und Klausel 5 (c) (oder beigefügtem Dokument bzw. Rechtsvorschrift) eingeführt hat:

Der Datenimporteur muss sich an die folgenden **technischen Sicherheitsmaßnahmen** halten, die in seinen Informationssicherheitsrichtlinien näher beschrieben sind:

Sicherheitsanforderungen

1 osapiens muss zu jeder Zeit sicherstellen, dass seine IT-Systeme für den Zweck der Sicherung der Kundendaten gemäß guter Industriepraxis und dieser Vereinbarung geeignet sind und regelmäßig gewartet und, falls erforderlich, aufgerüstet werden, um dies zu gewährleisten.

2 osapiens muss jederzeit die ISO/IEC27001 oder anderweitig eine gute Industriepraxis in Bezug auf den Datenschutz sowie die Implementierung und Wartung von Back-up-Systemen einhalten.

3 Wenn osapiens dem Kunden im Rahmen des Cloud-Service Zugang zu einem IT-System verschafft oder Kundendaten auf seinen eigenen Systemen oder den Systemen eines verbundenen Unternehmens, eines Unterauftragsverarbeiters oder eines Auftragnehmers speichert, muss osapiens jährlich Penetrationstests auf Anwendungs- bzw. Infrastrukturebene mit einem in Großbritannien ansässigen, unabhängigen und CREST-zertifizierten Auftragnehmer durchführen und den Kunden über die Ergebnisse dieser Tests informieren. Werden auf Wunsch des Kunden Penetrationstests durchgeführt, so trägt der Kunde die Kosten. Durch solche Penetrationstests identifizierte Abhilfemaßnahmen müssen von osapiens auf eigene Kosten durchgeführt werden.

4 osapiens muss (ohne Kosten für den Kunden):

4.1 alle Kundendaten wiederherstellen, neu kompilieren oder neu erstellen (zeitnah und gemäß guter Industriepraxis), die durch osapiens oder einen seiner Mitarbeiter infolge eines Datenschutzverstoßes verloren, gelöscht oder beschädigt wurden;

4.2 auf Verlangen des Kunden jederzeit eine Kopie aller oder eines Teils der Kundendaten, die sich zu diesem Zeitpunkt im Besitz, in der Obhut oder unter der Kontrolle der Agentur befinden und in elektronischer Form vorliegen, in dem vom Kunden gewünschten Format zur Verfügung stellen;

4.3 sicherstellen, dass die Löschung von Kundendaten auf sichere Weise erfolgt, so dass die Kundendaten nicht wiederhergestellt werden können;

4.4 die Sicherheit der Kundendaten so weit wie möglich wahren und jeglichen Verlust, Offenlegung, Diebstahl, Manipulation oder Abfangen von Kundendaten verhindern;

4.5 alle branchenüblichen Vorsichtsmaßnahmen ergreifen, um die Installation von Viren oder anderen nicht autorisierten Computerprogrammen in seinen Computersystemen oder die des Kunden verhindern und auf andere Weise die Beschädigung von Kundendaten vermeiden, und,

falls ein Virus oder ein solches anderes Programm in eines der Systeme des Kunden infolge einer Handlung oder Unterlassung von osapiens eindringt, den Kunden unverzüglich zu benachrichtigen und ihm alle erforderliche Unterstützung zu gewähren, um die Auswirkungen zu minimieren.

4.6 sicherstellen, dass alle Kundendaten, die auf einem tragbaren elektronischen Gerät (einschließlich Laptops, Speichersticks und Sicherungsbändern) gespeichert oder elektronisch übertragen werden, sicher verschlüsselt werden;

4.7 dafür sorgen, dass die Mitarbeiter von osapiens den Kunden unverzüglich informieren, wenn sie von einer unbefugten oder versehentlichen Offenlegung, einem Verlust oder einer Beschädigung von Kundendaten Kenntnis erlangen oder einen begründeten Verdacht haben; und

4.8 sicherstellen, dass regelmäßige Sicherungskopien der Kundendaten gemäß guter Industriepraxis (in jedem Fall mind. alle 30 Tage) erstellt und an einem sicheren physischen Ort getrennt von der primären Kopie der Kundendaten aufbewahrt werden.