

ALLGEMEINE GESCHÄFTSBEDINGUNGEN (AGB)

zwischen

HealthCare Consulting GmbH

Kolonitzgasse 2A/DG

1030 Wien

Österreich

Firmenbuch: FN 204710w

– nachfolgend „Anbieter“ oder „HCC“ –

und dem jeweiligen Unternehmenskunden

– nachfolgend „Kunde“ –

gemeinsam die „Parteien“.

1. GELTUNGSBEREICH UND VERTRAGSZWECK

- 1.1. Diese Allgemeinen Geschäftsbedingungen („AGB“) gelten für die Bereitstellung und Nutzung der Software-as-a-Service-Lösung Convilance durch Unternehmenskunden aus der Pharma-, Medizinprodukte-, Biotechnologie-, Life-Sciences- und verwandten regulierten Branchen.
- 1.2. Convilance richtet sich ausschließlich an Unternehmer. Eine Nutzung durch Verbraucher ist ausgeschlossen.
- 1.3. Convilance ist eine webbasierte Softwarelösung zur Unterstützung bei der Überwachung, Aggregation, Bearbeitung, Dokumentation und Weiterleitung von Informationen aus digitalen Kommunikationskanälen, insbesondere im Zusammenhang mit Pharmakovigilanz, Drug Safety, Product Safety, Post-Market-Surveillance und verwandten Compliance-Prozessen.

- 1.4. Diese AGB bilden zusammen mit den im Einzelfall vereinbarten Vertragsdokumenten den Vertrag zwischen den Parteien („Vertrag“).

2. VERTRAGSABSCHLUSS, VERTRAGSSTRUKTUR UND RANGFOLGE

- 2.1. Der Vertrag kommt durch Annahme des Angebots durch den Kunden innerhalb der darin angegebenen Bindungsfrist zustande. Der Anbieter ist während der im Angebot angegebenen Bindungsfrist an das Angebot gebunden. Sofern im Angebot keine Bindungsfrist angegeben ist, gilt eine Bindungsfrist von 14 Tagen als vereinbart.
- 2.2. Der Vertrag kann aus den folgenden Dokumenten bestehen:
 - a) Angebot,
 - b) diesen Allgemeinen Geschäftsbedingungen („AGB“),
 - c) Service Level Agreement („SLA“),
 - d) Auftragsverarbeitungsvereinbarung („AVV“),
 - e) Technischen und organisatorischen Maßnahmen („TOM“),
 - f) Optional: Statement of Work („SOW“) für Implementierungs-, Integrations- oder Beratungsleistungen.
- 2.3. Bei Widersprüchen gilt grundsätzlich folgende Rangfolge:
 1. individuell ausgehandelte Bestimmungen im Angebot oder SOW,
 2. diese AGB,
 3. AVV für datenschutzrechtliche Sachverhalte,
 4. SLA für Verfügbarkeit und Support,
 5. TOM für Informationssicherheitsanforderungen.
- 2.4. Abweichende Geschäfts- oder Einkaufsbedingungen des Kunden gelten nur, wenn der Anbieter ihnen ausdrücklich schriftlich zugestimmt hat.

3. BEREITSTELLUNG VON CONVILANCE

- 3.1. Der Anbieter stellt dem Kunden Convilance während der Vertragslaufzeit als browserbasierte SaaS-Lösung zur Verfügung.
- 3.2. Der konkrete Leistungsumfang ergibt sich aus dem Angebot. Darin können insbesondere festgelegt werden:
 - a) Organisationen und Gesellschaften des Kunden,
 - b) überwachte digitale Kanäle,
 - c) Benutzerzahl,
 - d) Support-Level,
 - e) zusätzliche Services.
- 3.3. Soweit nicht ausdrücklich vereinbart, schuldet der Anbieter keinen bestimmten wirtschaftlichen, medizinischen oder regulatorischen Erfolg.
- 3.4. Convilance wird über eine zentrale SaaS-Infrastruktur betrieben. Der Kunde hat keinen Anspruch auf Überlassung des Quellcodes oder Installation einer eigenen Softwarekopie.

4. IMPLEMENTIERUNG UND KONFIGURATION

- 4.1. Die Parteien wirken bei der Einführung von Convilance angemessen zusammen.
- 4.2. Der Anbieter unterstützt insbesondere bei der technischen Einrichtung, Anbindung der vereinbarten Kanäle und initialen Konfiguration entsprechend dem vereinbarten Leistungsumfang.
- 4.3. Der Kunde stellt rechtzeitig alle erforderlichen Informationen, Ansprechpartner, Berechtigungen, Zugangsdaten und sonstigen Mitwirkungsleistungen zur Verfügung.
- 4.4. Verzögerungen, die aufgrund fehlender oder verspäteter Mitwirkung des Kunden entstehen, verlängern vereinbarte Implementierungsfristen entsprechend.
- 4.5. Soweit der Anbieter kundenspezifische Entwicklungs-, Integrations-, Migrations- oder Beratungsleistungen erbringt, sollen diese in einem gesonderten SOW beschrieben werden.

5. VORGESEHENE VERWENDUNG UND VERANTWORTUNGSABGRENZUNG

- 5.1. Convilance dient als technisches Unterstützungswerkzeug für digitale Monitoring-, Screening-, Dokumentations- und Weiterleitungsprozesse.
- 5.2. Convilance kann insbesondere eingesetzt werden, um digitale Kommunikationskanäle automatisiert auf neue Inhalte zu überwachen, diese Inhalte zentral zur Verfügung zu stellen, Screening- und Bearbeitungsschritte zu dokumentieren und relevante Informationen an definierte Empfänger weiterzuleiten.
- 5.3. Convilance ersetzt keine medizinische, pharmazeutische, regulatorische oder rechtliche Beurteilung durch entsprechend qualifizierte Personen.
- 5.4. Soweit nicht in einem separaten SOW ausdrücklich anders vereinbart, bleibt der Kunde allein verantwortlich für:
 - a) die fachliche Bewertung von Informationen und Meldungen,
 - b) die Feststellung, ob eine Information eine Nebenwirkungsmeldung, eine Produktbeschwerde oder einen sonstigen regulatorisch relevanten Sachverhalt darstellt,
 - c) die Festlegung des regulatorischen „Day Zero“,
 - d) die Einhaltung gesetzlicher oder regulatorischer Meldefristen,
 - e) Meldungen an Behörden, Geschäftspartner, Lizenzpartner oder andere Stellen,
 - f) Follow-up-Aktivitäten,
 - g) medizinische Kodierung, Case Processing und medizinische Bewertung
 - h) seine Pharmakovigilanz-, Quality- und Compliance-Systeme insgesamt.
- 5.5. Automatisierte Relevanzbewertungen, Keywords, Filter, Priorisierungen oder vergleichbare Funktionen unterstützen die Bearbeitung durch den Kunden. Sie stellen keine verbindliche regulatorische Entscheidung dar.
- 5.6. Der Kunde bleibt dafür verantwortlich, Convilance entsprechend seinem regulatorischen Anwendungsfall zu konfigurieren und innerhalb seiner eigenen Prozesse ordnungsgemäß einzusetzen.

6. AUSGELAGERTE PHARMAKOVIGILANZ-AKTIVITÄTEN

- 6.1. Soweit der Anbieter aufgrund eines gesonderten SOW über die bloße technische Bereitstellung der Software hinaus Pharmakovigilanz-Aktivitäten im Auftrag des Kunden durchführt, sind diese Aktivitäten ausdrücklich im SOW zu beschreiben.
- 6.2. Ein solches SOW soll insbesondere festlegen:
 - a) Umfang der delegierten Aktivitäten,
 - b) Rollen und Verantwortlichkeiten der Parteien,
 - c) betroffene Produkte,
 - d) relevante Kommunikationskanäle,
 - e) Verfahren zum Austausch von Safety Data,
 - f) Übermittlungswege und Fristen,
 - g) Eskalationsprozesse,
 - h) Qualitätsanforderungen,
 - i) Audit- und Inspektionsanforderungen,
 - j) gegebenenfalls Reconciliation-Prozesse.
- 6.3. Soweit nach anwendbarem Pharmakovigilanzrecht erforderlich, stimmt der Anbieter Audit- und behördlichen Inspektionsrechten entsprechend Abschnitt 13 zu.
- 6.4. Die gesetzliche Verantwortung eines Zulassungsinhabers (Marketing Authorisation Holders / MAH), Herstellers oder sonstigen regulatorisch verantwortlichen Unternehmens wird durch die Beauftragung des Anbieters nicht auf diesen übertragen.

7. QUALIFIZIERUNG UND VALIDIERUNG

- 7.1. Der Anbieter betreibt Convilance unter Anwendung angemessener dokumentierter Entwicklungs-, Test-, Release- und Change-Management-Prozesse.
- 7.2. Soweit vereinbart, stellt der Anbieter dem Kunden angemessene vorhandene Dokumentationen zur Verfügung, die den Kunden bei seiner risikobasierten Bewertung, Lieferantenqualifizierung oder System-Validierung unterstützen können.

- 7.3. Art und Umfang eines gegebenenfalls bereitgestellten Validierungs- oder Qualifizierungs-Pakets werden in einem separaten SOW festgelegt.
- 7.4. Soweit nicht ausdrücklich schriftlich anders vereinbart, bleibt der Kunde verantwortlich für:
- a) die Definition seines Intended Use,
 - b) seine User Requirements,
 - c) seine regulatorische Einordnung des Systems,
 - d) die Durchführung und Dokumentation einer erforderlichen kundenseitigen Risikobewertung,
 - e) die Validierung seiner kundenspezifischen Konfiguration und Geschäftsprozesse.
- 7.5. Änderungen von Convilance werden entsprechend dem beim Anbieter geltenden Change-Management-Prozess bewertet, getestet und dokumentiert.

8. INFORMATIONSSICHERHEIT

- 8.1. Der Anbieter unterhält angemessene technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Convilance und der darin verarbeiteten Kundendaten.
- 8.2. Die wesentlichen Sicherheitsmaßnahmen können in den TOMs dokumentiert werden.
- 8.3. Die Sicherheitsmaßnahmen sollen, soweit für die vereinbarte Leistung angemessen, insbesondere folgende Bereiche berücksichtigen:
- a) Zugriffskontrolle und Berechtigungsmanagement,
 - b) Authentifizierung,
 - c) Verschlüsselung bei der Datenübertragung,
 - d) System- und Netzwerkabsicherung,
 - e) Logging und Monitoring,
 - f) Vulnerability- und Patch-Management,
 - g) Backup und Wiederherstellung,
 - h) Business Continuity,
 - i) Incident Management,
 - j) Secure Software Development,
 - k) Mitarbeiterberechtigungen und Vertraulichkeit.

- 8.4. Der Anbieter überprüft seine Sicherheitsmaßnahmen regelmäßig und darf diese dem Stand der Technik und der Risikolage entsprechend weiterentwickeln, sofern das vereinbarte Schutzniveau insgesamt nicht wesentlich reduziert wird.

9. SICHERHEITSEREIGNISSE

- 9.1. Der Anbieter unterhält einen angemessenen Prozess zur Erkennung, Bewertung, Behandlung und Dokumentation von Informationssicherheitsvorfällen.
- 9.2. Ein „Security Incident“ ist ein bestätigtes Sicherheitsereignis, das zu einer unbeabsichtigten oder unrechtmäßigen Vernichtung, einem Verlust, einer Veränderung, einer unbefugten Offenlegung oder einem unbefugten Zugriff auf Kundendaten führt oder voraussichtlich führen kann.
- 9.3. Der Anbieter informiert den Kunden über einen Security Incident, der Kundendaten wesentlich betrifft, unverzüglich und grundsätzlich innerhalb von 48 Stunden nach dessen Bestätigung, soweit eine solche Information gesetzlich zulässig ist.
- 9.4. Die Information soll, soweit zu diesem Zeitpunkt verfügbar, enthalten:
- a) Art des Vorfalls,
 - b) betroffene Systeme oder Datenkategorien,
 - c) bekannte oder erwartete Auswirkungen,
 - d) bereits ergriffene Gegenmaßnahmen,
 - e) geplante weitere Maßnahmen.
- 9.5. Der Anbieter stellt dem Kunden angemessene weitere Informationen zur Verfügung, soweit diese für gesetzliche Melde- oder Informationspflichten des Kunden erforderlich und beim Anbieter verfügbar sind.
- 9.6. Datenschutzverletzungen werden ergänzend nach Maßgabe der AVV behandelt.

10. DATENSCHUTZ

- 10.1. Jede Partei erfüllt die auf sie anwendbaren datenschutzrechtlichen Vorschriften.

- 10.2. Soweit der Anbieter personenbezogene Daten im Auftrag des Kunden verarbeitet, schließen die Parteien eine AVV gemäß Art. 28 DSGVO.
- 10.3. Der Kunde ist, soweit nicht ausdrücklich anders vereinbart, Verantwortlicher für die im Rahmen der Nutzung von Convilance verarbeiteten personenbezogenen Daten.
- 10.4. Dies gilt insbesondere für personenbezogene Informationen, die aus digitalen Kommunikationskanälen übernommen werden und Gesundheitsdaten oder andere besondere Kategorien personenbezogener Daten enthalten können.
- 10.5. Der Kunde bestimmt insbesondere:
 - a) die überwachten Kanäle,
 - b) die Zwecke der Verarbeitung,
 - c) Benutzer und Zugriffsrechte,
 - d) relevante Aufbewahrungszeiträume,
 - e) Anonymisierungs- und Löschfristen,
 - f) Empfänger von Weiterleitungen.
- 10.6. Der Kunde ist dafür verantwortlich, dass für die von ihm veranlasste Verarbeitung eine ausreichende datenschutzrechtliche Grundlage besteht.
- 10.7. Einzelheiten zu Subprozessoren, internationalen Datentransfers, Betroffenenrechten, Löschung und Sicherheitsereignissen werden in der AVV geregelt.

11. SUBUNTERNEHMER UND SUBPROZESSOREN

- 11.1. Der Anbieter darf zur Bereitstellung von Convilance geeignete verbundene Unternehmen und Subunternehmer einsetzen.
- 11.2. Soweit diese Subunternehmer personenbezogene Daten als Subprozessoren verarbeiten, gelten die Regelungen der AVV.
- 11.3. Der Anbieter bleibt gegenüber dem Kunden für die Erfüllung seiner vertraglichen Pflichten verantwortlich, soweit diese durch von ihm eingesetzte Subunternehmer erbracht werden.

- 11.4. Soweit der Anbieter ausdrücklich mit Pharmakovigilanz-Aktivitäten beauftragt wurde und eine Weitervergabe solcher Aktivitäten regulatorisch einer Zustimmung des Kunden bedarf, erfolgt eine solche Weitervergabe nur nach Maßgabe des betreffenden SOW und der anwendbaren regulatorischen Anforderungen.

12. DRITTPLATTFORMEN UND EXTERNE SCHNITTSTELLEN

- 12.1. Convillance kann Informationen aus Social-Media-Plattformen, Messaging-Diensten, App Stores, Webseiten, RSS-Feeds, digitalen Plattformen und anderen Systemen Dritter abrufen oder verarbeiten.
- 12.2. Die technische Verfügbarkeit solcher Daten kann von APIs, Schnittstellen, Zugriffsrechten, Nutzungsbedingungen, technischen Beschränkungen und Entscheidungen des jeweiligen Drittanbieters abhängig sein.
- 12.3. Der Anbieter hat keinen vollständigen Einfluss auf die dauerhafte Verfügbarkeit und Funktionsweise von Drittplattformen.
- 12.4. Der Anbieter übernimmt daher keine Garantie dafür, dass jeder über einen Drittanbieter veröffentlichte Inhalt jederzeit oder vollständig technisch abrufbar ist.
- 12.5. Wird eine Schnittstelle durch einen Drittanbieter wesentlich geändert oder eingestellt, wird der Anbieter wirtschaftlich angemessene Maßnahmen ergreifen, um die Anbindung anzupassen oder eine alternative technische Lösung bereitzustellen, soweit dies technisch und wirtschaftlich zumutbar ist.
- 12.6. Betrifft die Änderung eine für den Kunden wesentliche Funktion dauerhaft und kann keine angemessene Ersatzlösung bereitgestellt werden, werden die Parteien in gutem Glauben über eine Anpassung des betroffenen Leistungsumfangs beraten.

13. AUDIT- UND INSPEKTIONSRECHTE

- 13.1. Der Anbieter erkennt an, dass Kunden aus regulierten Branchen angemessene Lieferantenqualifizierungen und Audit-Anforderungen erfüllen müssen.

- 13.2. Der Anbieter stellt dem Kunden auf Anfrage zunächst vorhandene geeignete Audit-, Compliance-, Sicherheits- oder Qualifizierungs-Unterlagen zur Verfügung, soweit dies unter Berücksichtigung von Vertraulichkeit und Informationssicherheit angemessen ist.
- 13.3. Soweit diese Unterlagen zur Erfüllung berechtigter regulatorischer Anforderungen nicht ausreichen, kann der Kunde grundsätzlich einmal pro Kalenderjahr ein angemessenes Audit der für die Leistungserbringung relevanten Prozesse durchführen oder durch einen unabhängigen, zur Vertraulichkeit verpflichteten Dritten durchführen lassen.
- 13.4. Audits sind grundsätzlich mindestens 30 Tage im Voraus anzukündigen, während üblicher Geschäftszeiten durchzuführen und dürfen den Geschäftsbetrieb des Anbieters nicht unangemessen beeinträchtigen.
- 13.5. Soweit angemessen, sollen Remote-Audits oder dokumentenbasierte Audits Vorrang vor Vor-Ort-Audits haben.
- 13.6. Die Kosten kundenseitiger Audits trägt der Kunde. Zeigt ein Audit eine wesentliche, vom Anbieter zu vertretende Vertrags- oder Compliance-Verletzung, trägt der Anbieter seine eigenen angemessenen Kosten zur Behebung.
- 13.7. Audit-Rechte gewähren keinen Zugang zu:
 - a) Daten anderer Kunden,
 - b) Geschäftsgeheimnissen, die für das Audit nicht erforderlich sind,
 - c) Quellcode,
 - d) Informationen, deren Offenlegung Sicherheitsrisiken verursachen würde,
 - e) Informationen, deren Offenlegung gegenüber dem Kunden rechtlich unzulässig ist.
- 13.8. Gesetzliche oder behördliche Inspektionsrechte bleiben unberührt.
- 13.9. Soweit Convilance oder damit verbundene ausgelagerte Leistungen Gegenstand einer Inspektion einer zuständigen Arzneimittel- oder sonstigen Aufsichtsbehörde sind, wird der Anbieter im angemessenen Umfang mit dem Kunden und der zuständigen Behörde kooperieren.

14. SERVICE LEVELS, SUPPORT UND BUSINESS CONTINUITY

- 14.1. Verfügbarkeit, Supportzeiten, Prioritätsstufen und Reaktionszeiten werden in einem separaten Service-Level-Agreement (SLA) geregelt.
- 14.2. Ohne gesondertes SLA schuldet der Anbieter eine dem üblichen professionellen Betrieb einer B2B-SaaS-Lösung angemessene Verfügbarkeit, jedoch keine bestimmte prozentuale Mindestverfügbarkeit.
- 14.3. Von einer vereinbarten Verfügbarkeitsberechnung können insbesondere ausgenommen werden:
 - a) angekündigte Wartungsfenster,
 - b) Notfallwartung,
 - c) höhere Gewalt,
 - d) Ausfälle von Drittplattformen,
 - e) Ausfälle der kundenseitigen Infrastruktur,
 - f) vom Kunden verursachte Störungen.
- 14.4. Der Anbieter unterhält angemessene Vorkehrungen für Backup, Wiederherstellung und Business Continuity.
- 14.5. Konkrete Recovery Time Objectives („RTO“) und Recovery Point Objectives („RPO“) gelten nur, wenn diese ausdrücklich im SLA festgelegt wurden.

15. CHANGE MANAGEMENT UND PRODUKTWEITERENTWICKLUNG

- 15.1. Der Anbieter ist berechtigt und verpflichtet, Convilance laufend weiterzuentwickeln, insbesondere zur:
 - a) Verbesserung von Funktionalität und Benutzerfreundlichkeit,
 - b) Behebung von Fehlern,
 - c) Verbesserung der Sicherheit,
 - d) Anpassung an technische Entwicklungen,
 - e) Anpassung an Änderungen von Drittplattformen,
 - f) Umsetzung rechtlicher oder regulatorischer Anforderungen.

- 15.2. Änderungen dürfen die wesentlichen vereinbarten Nutzungsmöglichkeiten während einer festen Vertragsperiode nicht ohne sachlichen Grund erheblich reduzieren.
- 15.3. Wesentliche Änderungen, die voraussichtlich erhebliche Auswirkungen auf einen regulatorisch relevanten Workflow des Kunden haben, werden dem Kunden mit angemessenem Vorlauf angekündigt, soweit dies technisch und regulatorisch möglich ist.
- 15.4. Sicherheitskritische Änderungen oder Änderungen aufgrund kurzfristiger Vorgaben von Drittplattformen dürfen erforderlichenfalls ohne vorherige Ankündigung umgesetzt werden.

16. PFLICHTEN DES KUNDEN

- 16.1. Der Kunde nutzt Convillance ausschließlich entsprechend dem Vertrag und dem vereinbarten Zweck.
- 16.2. Um die Plattform im vollen Umfang nutzen zu können, muss der Kunde die jeweils aktuellen Browser-Technologien verwenden oder deren Verwendung ermöglichen. Bei Verwendung älterer Technologien kann es sein, dass der Kunde die Plattform nicht im vollen Umfang nutzen kann.
- 16.3. Der Kunde ist insbesondere verantwortlich für:
 - a) Auswahl der zu überwachenden digitalen Kanäle,
 - b) Einholung erforderlicher Zugangs- und Nutzungsrechte,
 - c) Definition von Benutzerrechten,
 - d) Vertretungs- und Eskalationsregeln,
 - e) Konfiguration regulatorischer Workflows,
 - f) regelmäßige Überprüfung seiner Konfiguration,
 - g) Bearbeitung eingehender Meldungen,
 - h) Einhaltung regulatorischer Fristen,
 - i) angemessene Business-Continuity-Prozesse auf Kundenseite.
- 16.4. Der Kunde gewährleistet, dass Zugangsdaten nicht unberechtigt weitergegeben werden und nur autorisierte Benutzer Zugriff erhalten.
- 16.5. Der Kunde informiert den Anbieter unverzüglich über ihm bekannte unbefugte Zugriffe oder Sicherheitsprobleme im Zusammenhang mit seinen Benutzerkonten.

16.6. Der Kunde stellt den Anbieter von Ansprüchen Dritter frei, soweit diese darauf beruhen, dass der Kunde schuldhaft gegen seine Verpflichtungen aus dem Vertrag oder gegen anwendbares Recht verstößt. Dies gilt insbesondere für Ansprüche, die daraus entstehen, dass

- a) vom Kunden bereitgestellte oder zur Verarbeitung veranlasste Daten, Inhalte oder Informationen Rechte Dritter verletzen,
- b) der Kunde nicht über die erforderlichen Rechte, Berechtigungen oder sonstigen Rechtsgrundlagen für die Überwachung, Erhebung, Verarbeitung oder Weiterleitung von Daten oder Inhalten verfügt,
- c) Convilance durch den Kunden oder durch ihm zurechenbare Nutzer vertragswidrig oder rechtswidrig genutzt wird, oder
- d) vom Kunden erteilte Weisungen oder vorgegebene Konfigurationen gegen anwendbare datenschutzrechtliche, regulatorische oder sonstige gesetzliche Anforderungen verstoßen.

Die Freistellung umfasst, soweit gesetzlich zulässig, auch angemessene und erforderliche Kosten der Rechtsverteidigung. Sie gilt nicht, soweit der betreffende Anspruch durch eine Pflichtverletzung des Anbieters verursacht oder mitverursacht wurde.

Der Anbieter wird den Kunden über einen solchen Anspruch unverzüglich informieren und ihm, soweit rechtlich und tatsächlich möglich, angemessene Gelegenheit geben, an der Abwehr oder Beilegung des Anspruchs mitzuwirken. Der Anbieter darf ohne vorherige Zustimmung des Kunden keinen Vergleich schließen, der dem Kunden eine Zahlungspflicht, ein Schuldanerkenntnis oder sonstige wesentliche Verpflichtungen auferlegt; die Zustimmung darf nicht unbillig verweigert werden.

17. KUNDENDATEN

- 17.1. Sämtliche Rechte an den vom Kunden bereitgestellten Kundendaten verbleiben beim Kunden bzw. den jeweiligen Rechteinhabern.
- 17.2. Der Kunde räumt dem Anbieter die für die Vertragserfüllung technisch erforderlichen, nicht ausschließlichen Rechte zur Verarbeitung, Speicherung, Übertragung, Vervielfältigung und Sicherung der Kundendaten ein.
- 17.3. Eine Nutzung personenbezogener Kundendaten zu eigenen Zwecken des Anbieters erfolgt nur, soweit hierfür eine gesetzliche Grundlage besteht oder dies mit dem Kunden ausdrücklich vereinbart wurde.

- 17.4. Der Anbieter darf aggregierte oder hinreichend anonymisierte technische Nutzungsinformationen zur Sicherheit, Fehleranalyse, Kapazitätsplanung und Verbesserung des Dienstes verwenden, sofern weder der Kunde noch natürliche Personen daraus identifiziert werden können.

18. GEISTIGES EIGENTUM

- 18.1. Sämtliche Rechte an Convilance, einschließlich Software, Architektur, Benutzeroberfläche, Datenbankstruktur, Dokumentation, Marken und zugrunde liegendem Know-how, verbleiben beim Anbieter oder seinen Lizenzgebern.
- 18.2. Der Anbieter räumt dem Kunden für die Vertragslaufzeit ein nicht ausschließliches, nicht übertragbares und auf den vereinbarten Umfang beschränktes Nutzungsrecht an Convilance ein.
- 18.3. Der Kunde darf Convilance insbesondere nicht:
- a) vervielfältigen oder vertreiben,
 - b) Dritten außerhalb des zulässigen Nutzerkreises bereitstellen,
 - c) Schutzmechanismen umgehen,
 - d) zurückentwickeln, außer soweit zwingendes Recht dies gestattet,
 - e) zur Entwicklung eines konkurrierenden Produkts systematisch technisch auswerten.
- 18.4. Feedback und Verbesserungsvorschläge des Kunden dürfen vom Anbieter zur Weiterentwicklung von Convilance verwendet werden, sofern dabei keine vertraulichen Informationen des Kunden offengelegt werden.

19. SCHUTZRECHTE DRITTER

- 19.1. Der Anbieter steht dafür ein, dass die vertragsgemäße Nutzung von Convilance nach seinem Kenntnisstand keine Schutzrechte Dritter verletzt.
- 19.2. Wird gegen den Kunden wegen der vertragsgemäßen Nutzung von Convilance ein begründeter Anspruch wegen Verletzung von Schutzrechten Dritter geltend gemacht, kann der Anbieter nach eigener Wahl:
- a) die erforderlichen Rechte beschaffen,

- b) die betroffene Leistung so ändern, dass keine Verletzung mehr besteht,
- c) eine funktional angemessene Ersatzlösung bereitstellen.

- 19.3. Ist keine dieser Maßnahmen wirtschaftlich zumutbar, kann der Anbieter den betroffenen Leistungsteil beenden und bereits im Voraus gezahlte Gebühren für den nicht mehr nutzbaren Zeitraum anteilig erstatten.
- 19.4. Dies gilt nicht, soweit der Anspruch auf Kundendaten, kundenseitigen Vorgaben, nicht autorisierten Änderungen oder einer Nutzung entgegen dem Vertrag beruht.

20. VERTRAULICHKEIT

- 20.1. Jede Partei behandelt vertrauliche Informationen der anderen Partei streng vertraulich und verwendet diese ausschließlich zur Durchführung des Vertrags.
- 20.2. Vertrauliche Informationen umfassen insbesondere:
- a) Geschäfts- und Betriebsgeheimnisse,
 - b) technische Dokumentationen,
 - c) Sicherheitsdokumentationen,
 - d) Audit-Berichte,
 - e) Preis- und Vertragsinformationen,
 - f) regulatorische Dokumentationen,
 - g) Produktstrategien,
 - h) Kundendaten.
- 20.3. Die Weitergabe an Mitarbeiter, verbundene Unternehmen, professionelle Berater und Unterauftragnehmer ist zulässig, soweit diese die Informationen zur Vertragserfüllung benötigen und angemessenen Vertraulichkeitspflichten unterliegen.
- 20.4. Die Vertraulichkeitsverpflichtung gilt nicht für Informationen, die nachweislich:
- a) öffentlich bekannt sind,
 - b) der empfangenden Partei bereits rechtmäßig bekannt waren,
 - c) rechtmäßig von einem Dritten erlangt wurden,

d) unabhängig entwickelt wurden.

- 20.5. Gesetzlich oder behördlich erforderliche Offenlegungen bleiben zulässig. Soweit rechtlich möglich, wird die andere Partei vorher informiert.
- 20.6. Die Verpflichtungen gelten fünf Jahre nach Vertragsende fort; Geschäftsgeheimnisse sind darüber hinaus entsprechend den gesetzlichen Anforderungen zu schützen.

21. VERGÜTUNG UND ZAHLUNGSBEDINGUNGEN

- 21.1. Gebühren, Abrechnungsmodell und Zahlungsintervalle ergeben sich aus dem Angebot.
- 21.2. Alle Preise verstehen sich in Euro zuzüglich gesetzlich anfallender Steuern und Abgaben.
- 21.3. Rechnungen sind, soweit nicht anders vereinbart, innerhalb von 30 Tagen ab Rechnungsdatum ohne Abzug fällig. Bankspesen bei Zahlungen in einer Fremdwährung sind vom Kunden zu tragen.
- 21.4. Bei Zahlungsverzug gelten die gesetzlichen Verzugszinsen für Unternehmergeschäfte.
- 21.5. Eine Aufrechnung durch den Kunden ist nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig, soweit gesetzlich zulässig.
- 21.6. Preise innerhalb einer festen Vertragsperiode werden grundsätzlich nicht erhöht, sofern keine Änderung des Leistungsumfangs vereinbart wird.
- 21.7. Preisänderungen für Verlängerungsperioden werden mit angemessenem Vorlauf vor Beginn der jeweiligen Verlängerungsperiode mitgeteilt.

22. GEWÄHRLEISTUNG

- 22.1. Der Anbieter gewährleistet, dass Convilance im Wesentlichen entsprechend der vereinbarten Leistungsbeschreibung funktioniert.

- 22.2. Der Kunde meldet wesentliche Fehler unverzüglich mit einer ausreichenden Beschreibung, damit der Anbieter diese nachvollziehen kann.
- 22.3. Der Anbieter behebt reproduzierbare, von ihm zu vertretende wesentliche Fehler innerhalb einer unter Berücksichtigung ihrer Kritikalität angemessenen Frist.
- 22.4. Keine Gewährleistung besteht für Störungen, die insbesondere verursacht werden durch:
- a) kundenseitige Systeme,
 - b) nicht unterstützte Software oder Hardware,
 - c) Fehlkonfiguration durch den Kunden,
 - d) mangelnde Mitwirkung,
 - e) unbefugte Änderungen,
 - f) Drittplattformen,
 - g) höhere Gewalt.
- 22.5. Der Anbieter gewährleistet nicht, dass automatisierte Such-, Filter- oder Relevanzfunktionen jeden regulatorisch relevanten Inhalt mit hundertprozentiger Genauigkeit identifizieren.

23. HAFTUNG

- 23.1. Der Anbieter haftet unbeschränkt:
- a) für vorsätzlich oder grob fahrlässig verursachte Schäden,
 - b) für Personenschäden,
 - c) nach zwingenden gesetzlichen Haftungs Vorschriften, soweit eine Haftungsbeschränkung gesetzlich unzulässig ist.
- 23.2. Bei leichter Fahrlässigkeit haftet der Anbieter nur für die Verletzung wesentlicher Vertragspflichten und nur für den bei Vertragsschluss typischerweise vorhersehbaren Schaden.
- 23.3. Soweit gesetzlich zulässig, ist die Haftung des Anbieters nach Ziffer 23.2 je Vertragsjahr insgesamt auf 100 % der vom Kunden in den zwölf Monaten vor dem haftungsauslösenden Ereignis gezahlten oder geschuldeten Netto-SaaS-Gebühren begrenzt.

23.4. Soweit gesetzlich zulässig, haftet keine Partei bei leichter Fahrlässigkeit für:

- a) entgangenen Gewinn,
- b) entgangene Einsparungen,
- c) mittelbare Schäden,
- d) reine Folgeschäden,
- e) Verlust von Geschäftsmöglichkeiten.

23.5. Die Haftungsbegrenzungen gelten entsprechend zugunsten von Organen, Mitarbeitern und Erfüllungsgehilfen des Anbieters.

23.6. Der Kunde bleibt insbesondere verantwortlich für Schäden, die daraus entstehen, dass regulatorisch relevante Meldungen nach Bereitstellung durch Convilance nicht oder nicht rechtzeitig fachlich bearbeitet, bewertet oder weitergemeldet werden.

24. COMPLIANCE

24.1. Jede Partei hält die auf sie anwendbaren Gesetze und Vorschriften ein.

24.2. Die Parteien verpflichten sich insbesondere zur Einhaltung anwendbarer Vorschriften zu:

- a) Datenschutz,
- b) Korruptionsbekämpfung,
- c) Geldwäscheprävention, soweit anwendbar,
- d) Exportkontrolle,
- e) Wirtschaftssanktionen,
- f) Wettbewerb und Kartellrecht.

24.3. Keine Partei ist verpflichtet, eine Leistung zu erbringen, wenn dies gegen anwendbare Sanktions- oder Exportkontrollvorschriften verstoßen würde.

25. VERTRAGSLAUFZEIT UND KÜNDIGUNG

- 25.1. Vertragsbeginn, Mindestvertragsdauer und Bedingungen bei einer Vertragsverlängerung ergeben sich aus dem Angebot.
- 25.2. Eine automatische Verlängerung findet nur statt, wenn sie im Angebot ausdrücklich vorgesehen ist.
- 25.3. Während einer vereinbarten Mindestvertragsdauer ist eine ordentliche Kündigung ausgeschlossen, sofern im Angebot nichts Abweichendes vereinbart ist.
- 25.4. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.
- 25.5. Ein wichtiger Grund liegt insbesondere vor, wenn eine Partei:
 - a) eine wesentliche Vertragspflicht verletzt und diese Verletzung trotz schriftlicher Aufforderung nicht innerhalb von grundsätzlich 30 Tagen behebt,
 - b) zahlungsunfähig wird oder ein Insolvenzverfahren eröffnet wird, soweit eine Kündigung gesetzlich zulässig ist,
 - c) wiederholt schwerwiegende Sicherheits- oder Compliance-Verstöße verursacht.
- 25.6. Bei einer nicht behebbaren wesentlichen Vertragsverletzung ist keine Nachfrist erforderlich.

26. SUSPENDIERUNG

- 26.1. Der Anbieter kann den Zugang zu Convilance ganz oder teilweise vorübergehend sperren, wenn dies erforderlich ist, um:
 - a) eine erhebliche Sicherheitsgefährdung abzuwenden,
 - b) rechtswidrige Nutzung zu verhindern,
 - c) erhebliche Schäden für andere Kunden oder Systeme zu verhindern,
 - d) einer gesetzlichen oder behördlichen Anordnung nachzukommen.
- 26.2. Bei Zahlungsverzug ist eine Suspendierung erst nach angemessener vorheriger Mahnung zulässig.

- 26.3. Der Anbieter wird den Kunden vor einer Suspendierung informieren, soweit dies unter Berücksichtigung der Dringlichkeit und rechtlicher Anforderungen möglich ist.
- 26.4. Eine Suspendierung wird auf den sachlich erforderlichen Umfang und Zeitraum beschränkt.

27. VERTRAGSENDE UND DATENEXPORT

- 27.1. Nach Vertragsende endet das Recht des Kunden zur Nutzung von Convilance.
- 27.2. Der Kunde kann während der Vertragslaufzeit verfügbare Export- und Reporting-Funktionen nutzen, um relevante Daten und Dokumentationen zu sichern.
- 27.3. Soweit nicht anders vereinbart, hält der Anbieter Kundendaten nach Vertragsende für einen Zeitraum von 60 Tagen für eine vereinbarte Datenherausgabe verfügbar.
- 27.4. Danach werden Kundendaten entsprechend den vereinbarten Löschregelungen gelöscht oder anonymisiert, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- 27.5. Benötigt der Kunde zusätzliche Exit-, Migration- oder Datenextraktionsleistungen, können diese auf Basis eines gesonderten SOW gegen angemessene Vergütung erbracht werden.
- 27.6. Soweit regulatorisch erforderliche Dokumentationen oder Audit-Unterlagen betroffen sind, werden die Parteien angemessene Regelungen über deren Aufbewahrung oder Herausgabe treffen.

28. HÖHERE GEWALT

- 28.1. Keine Partei haftet für eine Verzögerung oder Nichterfüllung, soweit diese auf einem Ereignis außerhalb ihres angemessenen Einflussbereichs beruht.
- 28.2. Dazu können insbesondere gehören:
 - a) Naturkatastrophen,
 - b) Krieg oder Terrorismus,
 - c) großflächige Energie- oder Telekommunikationsausfälle,

- d) behördliche Maßnahmen,
- e) erhebliche Cyberangriffe trotz angemessener Schutzmaßnahmen,
- f) Arbeitskämpfe,
- g) vergleichbare außergewöhnliche Ereignisse.

28.3. Die betroffene Partei informiert die andere Partei soweit möglich über wesentliche Auswirkungen und ergreift angemessene Maßnahmen zur Schadensbegrenzung.

29. ABTRETUNG UND CHANGE OF CONTROL

- 29.1. Keine Partei darf den Vertrag ohne vorherige Zustimmung der anderen Partei vollständig auf einen Dritten übertragen, wobei die Zustimmung nicht unbillig verweigert werden darf.
- 29.2. Eine Übertragung an ein verbundenes Unternehmen oder im Zusammenhang mit einer Verschmelzung, Umstrukturierung oder Veräußerung des betreffenden Geschäftsbetriebs ist zulässig, sofern der Rechtsnachfolger die vertraglichen Verpflichtungen übernimmt und keine berechtigten Interessen der anderen Partei entgegenstehen.

30. ÄNDERUNGEN DES VERTRAGS

- 30.1. Änderungen individuell ausgehandelter Vertragsbedingungen bedürfen der Schriftform.
- 30.2. Der Anbieter darf diese AGB für zukünftige Vertragsperioden ändern.
- 30.3. Wesentliche Änderungen werden dem Kunden mit angemessenem Vorlauf mitgeteilt.
- 30.4. Während einer festen Vertragsperiode werden wesentliche nachteilige Änderungen nur vorgenommen, wenn:
 - a) der Kunde zustimmt,
 - b) eine Änderung gesetzlich oder regulatorisch erforderlich ist oder
 - c) sie erforderlich ist, um eine erhebliche Sicherheitsgefährdung zu beheben.

31. SCHLUSSBESTIMMUNGEN

- 31.1. Diese AGBs bilden gemeinsam mit dem Angebot sowie den ausdrücklich einbezogenen Vertragsdokumenten die vollständige Vereinbarung der Parteien hinsichtlich seines Gegenstands.
- 31.2. Sollten einzelne Bestimmungen unwirksam oder undurchführbar sein, bleiben die übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung treten die gesetzlichen Regelungen.
- 31.3. Verzichtet eine Partei in einem Einzelfall auf die Durchsetzung eines Rechts, stellt dies keinen allgemeinen Verzicht auf dieses Recht dar.
- 31.4. Es gilt österreichisches Recht unter Ausschluss seiner Kollisionsnormen und des UN-Kaufrechts.
- 31.5. Erfüllungsort für Lieferungen und Leistungen von Convilance ist der Sitz des Anbieters.
- 31.6. Für sämtliche Streitigkeiten aus oder im Zusammenhang mit dem Vertrag wird, soweit gesetzlich zulässig, die ausschließliche Zuständigkeit des sachlich zuständigen Gerichts in Wien, Österreich, vereinbart.

Stand: Jänner 2025 / Convilance_AGB_V2_2025-01