VERTRAG ZUR AUFTRAGSVERARBEITUNG (AV-Vertrag)
Dieser Vertrag zur Auftragsverarbeitung (AV-Vertrag) wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter abgeschlossen und ist Bestandteil und unterliegt den Regelungen des Hauptvertrags.

---

1. Definitionen

Sofern in diesem AV-Vertrag nicht anders definiert, haben folgende Begriffe die hier festgelegte Bedeutung:

- **„Aufsichtsbehörde“**:
  Eine Regierungsbehörde mit bindender rechtlicher Befugnis über eine Partei.
- **„Auftragsverarbeiter“**:
  Das Unternehmen, einschließlich eines etwaigen „service providers“ im Sinne der US-Bundesstaatengesetze zum Datenschutz.
- **„AV-Vertrag“**:
  Dieser Vertrag zur Auftragsverarbeitung zusammen mit den Anhängen A und B.
- **„Betroffener“**:
  Hat die im Datenschutzrecht verwendete Bedeutung und schließt die Begriffe “data subject” „consumer“ oder „individual“ mit ein.
- **„Datenschutzrecht“**:
  Alle geltenden Gesetze und Regelungen, einschließlich der Gesetze und Regelungen der Europäischen Union, des Europäischen Wirtschaftsraums, ihrer Mitgliedstaaten und des Vereinigten Königreichs sowie aller Änderungen, Ersetzungen oder Verlängerungen derselben, die für die Verarbeitung personenbezogener Daten gelten, insofern diese anwendbar sind. Dazu gehören unter anderem:
  - die Datenschutz-, Privatsphäre- und elektronische Kommunikationsverordnung (EU Exit) von 2020,
  - die EU-DSGVO,
  - die UK-DSGVO,
  - das britische Datenschutzgesetz von 2018,
  - das FADP,
  - US-Bundesstaatengesetze zum Datenschutz
  - und alle geltenden nationalen Umsetzungsgesetze, Regelungen und nachrangigen Gesetze, die sich auf die Verarbeitung personenbezogener Daten und den Schutz der Vertraulichkeit elektronischer Kommunikation beziehen, einschließlich der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) und der Datenschutzverordnungen für elektronische Kommunikation (EU-Richtlinie) (SI 2003/2426).
- **„Eingeschränkte Übermittlung“**:
  Bedeutet:
  - Eine Übermittlung personenbezogener Daten über die Services vom EWR in ein Land oder an einen Empfänger außerhalb des EWR, das/der keiner Angemessenheitsentscheidung der Europäischen Kommission unterliegt (sofern die EU-DSGVO gilt).
  - Eine Übermittlung personenbezogener Daten über die Services aus dem Vereinigten Königreich an ein Land oder einen Empfänger außerhalb des Vereinigten Königreichs, das/der keiner Angemessenheitsregelung gemäß

Abschnitt 17A des britischen Datenschutzgesetzes von 2018 unterliegt (sofern die UK-DSGVO gilt).
    - Eine Übermittlung personenbezogener Daten über die Services aus der Schweiz in ein Land oder an einen Empfänger außerhalb des EWR und/oder der Schweiz, das/der keiner Angemessenheitsentscheidung der Europäischen Kommission unterliegt.
- **„EU-DSGVO“**:
  Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung).
- **„EWR“**:
  Der Europäische Wirtschaftsraum.
- **„FADP“**:
  Das schweizerische Bundesgesetz über den Datenschutz vom 1. September 2023, in seiner jeweils gültigen Fassung.
- **„Hauptvertrag“**:
  Der zwischen dem Verantwortlichen und dem Auftragsverarbeiter zur Erbringung der Services geschlossene Vertrag (Allgemeine Geschäftsbedingungen).
- **„Kundendaten“**:
  Alle Daten, die zum Zweck der Nutzung der Services durch den Kunden oder seiner autorisierten Nutzer vom Auftragsverarbeiter verarbeitet werden.
- **„Verbundenes Unternehmen“**:
  Jedes Unternehmen, das direkt oder indirekt eine Partei kontrolliert, von einer Partei kontrolliert wird oder unter gemeinsamer Kontrolle mit einer Partei steht. „Kontrolle“ im Sinne dieser Definition bedeutet direktes oder indirektes Eigentum oder Kontrolle über mehr als 50 % der Stimmrechte einer Partei.
- **„Personenbezogene Daten“**:
  Hat die im Datenschutzrecht verwendete Bedeutung und umfasst „persönlich identifizierbare Informationen“, wie dieser Begriff in den US-Bundesstaatengesetzen zum Datenschutz definiert ist.
- **„SCCs“** (Standardvertragsklauseln):
    - Die Standardvertragsklauseln der EU gemäß Artikel 46(2)(c) der EU-DSGVO.
    - Die Standardvertragsklauseln des Vereinigten Königreichs gemäß Artikel 46(2)(c) der UK-DSGVO.
    - Die für die Schweiz angepassten EU-Standardvertragsklauseln.
- **„Services“**:
  Alle vom Auftragsverarbeiter im Rahmen des Hauptvertrags bereitgestellten Dienste und Softwarelösungen.
- **„UK-DSGVO“**:
  Die EU-DSGVO, wie sie als Teil des Rechts von England und Wales, Schottland und Nordirland durch Abschnitt 3 des European Union (Withdrawal) Act 2018 gilt.
- **„Unterauftragsverarbeiter“**:
  Jede dritte Partei, die vom Auftragsverarbeiter direkt oder indirekt mit der Verarbeitung personenbezogener Daten beauftragt wird.
- **„US-Bundesstaatengesetze zum Datenschutz“**:
  Datenschutzgesetze und -vorschriften von US-Bundesstaaten, einschließlich:
    - California Consumer Privacy Act (CCPA),
    - California Privacy Rights Act (CPRA),
    - Virginia Consumer Data Protection Act (VCDPA),
    - Colorado Privacy Act (CPA),

    - Connecticut Data Privacy Act (CTDPA),
    - Utah Consumer Privacy Act (UCPA),
    - Montana Consumer Data Privacy Act (MCDPA),
      und deren jeweilige Änderungen oder Ersetzungen.
- **„Verantwortlicher“**:
  Der Kunde.

---

2. Zweck

2.1 Der Auftragsverarbeiter hat sich verpflichtet, dem Verantwortlichen die Services gemäß den Bedingungen des Hauptvertrags bereitzustellen. Im Rahmen der Erbringung der Services verarbeitet der Auftragsverarbeiter Kundendaten im Auftrag des Verantwortlichen. Kundendaten können personenbezogene Daten enthalten. Der Auftragsverarbeiter wird diese personenbezogenen Daten gemäß den Bestimmungen dieses AV-Vertrags verarbeiten und schützen.

---

3. Umfang

3.1 Bei der Erbringung der Services für den Verantwortlichen gemäß den Bedingungen des Hauptvertrags wird der Auftragsverarbeiter personenbezogene Daten nur insoweit verarbeiten, wie dies für die Bereitstellung der Services gemäß der Regelungen des Hauptvertrags, dieses AV-Vertrags und den Anweisungen des Verantwortlichen, die im Hauptvertrag und diesem AV-Vertrag dokumentiert und von Zeit zu Zeit aktualisiert werden, erforderlich ist.

3.2 Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass jede natürliche Person, die im Auftrag des Verantwortlichen oder des Auftragsverarbeiters handelt und Zugang zu personenbezogenen Daten hat, diese Daten nur auf Anweisung des Verantwortlichen verarbeitet, es sei denn, sie ist aufgrund des Datenschutzrechts dazu verpflichtet.

---

4. Pflichten des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter darf personenbezogene Daten nur im Rahmen dieses AV-Vertrags erheben, verarbeiten oder verwenden.

4.2 Der Auftragsverarbeiter bestätigt, dass er personenbezogene Daten im Auftrag des Verantwortlichen gemäß den dokumentierten Anweisungen des Verantwortlichen verarbeitet.

4.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass eine der Anweisungen des Verantwortlichen zur Verarbeitung personenbezogener Daten gegen das Datenschutzrecht verstößt.

4.4 Der Auftragsverarbeiter stellt sicher, dass alle Mitarbeiter, Vertreter, Beauftragten und Auftragnehmer, die mit der Verarbeitung personenbezogener Daten befasst sind:
(i) über die vertrauliche Natur der personenbezogenen Daten informiert sind und vertraglich zur Vertraulichkeit verpflichtet werden;
(ii) angemessen in ihren Verantwortlichkeiten als Auftragsverarbeiter geschult sind; und
(iii) an die Bedingungen dieses AV-Vertrags gebunden sind.

4.5 Der Auftragsverarbeiter implementiert geeignete technische und organisatorische Maßnahmen, um personenbezogene Daten zu schützen, wobei Folgendes berücksichtigt wird:
(i) den Stand der Technik;
(ii) die Implementierungskosten;
(iii) die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung; sowie
(iv) die Wahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten betroffener natürlicher Personen.

4.6 Der Auftragsverarbeiter implementiert geeignete technische und organisatorische Maßnahmen, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko angemessen ist. Dazu gehören unter anderem:
(i) Pseudonymisierung und Verschlüsselung personenbezogener Daten;
(ii) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten aufrechtzuerhalten;
(iii) die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Vorfalls rechtzeitig wiederherzustellen; und
(iv) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Sicherstellung der Verarbeitungssicherheit.
Beim Festlegen des angemessenen Sicherheitsniveaus wird insbesondere das Risiko berücksichtigt, das durch die Verarbeitung entsteht, insbesondere durch unbeabsichtigte oder unrechtmäßige Zerstörung, Verlust, Veränderung, unbefugte Offenlegung von oder Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten.

4.7 Die im Anhang B beschriebenen technischen und organisatorischen Maßnahmen gelten stets als Mindeststandard für die Sicherheit. Der Verantwortliche akzeptiert, dass diese Maßnahmen entwickelt und überprüft werden können und der Auftragsverarbeiter alternative geeignete Maßnahmen verwenden darf, sofern diese den im Anhang B beschriebenen Standards entsprechen und die Pflichten des Auftragsverarbeiters gemäß den Klauseln 4.5 und 4.6 erfüllen.

4.8 Der Verantwortliche erkennt an, dass der Auftragsverarbeiter im Rahmen der Bereitstellung der Services Zugriff auf personenbezogene Daten haben muss, um technische Probleme zu lösen, Anfragen des Verantwortlichen zu beantworten und den ordnungsgemäßen Betrieb der Services sicherzustellen. Dieser Zugriff wird auf diese Zwecke beschränkt.

4.9 Unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Pflichten des Verantwortlichen in Bezug auf Anfragen zur Ausübung der Rechte Betroffener und der Einhaltung der datenschutzrechtlichen Pflichten des Verantwortlichen.

4.10 Der Auftragsverarbeiter bestätigt, dass er und/oder seine verbundenen Unternehmen einen Datenschutzbeauftragten ernannt haben, sofern dies durch das Datenschutzrecht vorgeschrieben ist. Der Datenschutzbeauftragte ist per E-Mail unter DPO@QUIXXS.com erreichbar.

4.11 Der Auftragsverarbeiter darf:
(i) keine personenbezogenen Daten verkaufen;
(ii) personenbezogene Daten nicht zu kommerziellen Zwecken nutzen oder offenlegen, die über die Bereitstellung der Services gemäß der Regelungen des Hauptvertrags hinausgehen; und
(iii) personenbezogene Daten nicht außerhalb der Regelungen des Hauptvertrags speichern, nutzen oder offenlegen.

---

5. Pflichten des Verantwortlichen

5.1 Der Verantwortliche erklärt und garantiert, dass:
(i) er diesen AV-Vertrag und seine Pflichten gemäß dem Datenschutzrecht einhält;
(ii) er alle erforderlichen Genehmigungen, Einwilligungen und Autorisierungen eingeholt hat, um dem Auftragsverarbeiter, seinen verbundenen Unternehmen und Unterauftragsverarbeitern zu gestatten, ihre Rechte auszuüben oder ihre Pflichten gemäß diesem AV-Vertrag zu erfüllen; und
(iii) alle verbundenen Unternehmen des Verantwortlichen, die die Services nutzen, die in diesem AV-Vertrag festgelegten Pflichten des Verantwortlichen einhalten.

5.2 Der Verantwortliche implementiert geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, unter Berücksichtigung von:
(i) dem Stand der Technik;
(ii) den Implementierungskosten;
(iii) der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung; und
(iv) der Wahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten betroffener natürlicher Personen.

5.3 Der Verantwortliche implementiert geeignete technische und organisatorische Maßnahmen, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko angemessen ist, einschließlich, aber nicht beschränkt auf:
(i) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
(ii) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten aufrechtzuerhalten;
(iii) die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Vorfalls rechtzeitig wiederherzustellen; und
(iv) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Sicherstellung der Verarbeitungssicherheit.
Bei der Festlegung des angemessenen Sicherheitsniveaus werden insbesondere die Risiken berücksichtigt, die durch die Verarbeitung entstehen, insbesondere durch unbeabsichtigte oder unrechtmäßige Zerstörung, Verlust, Veränderung, unbefugte Offenlegung von oder Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten.

5.4 Der Verantwortliche erkennt an und stimmt zu, dass bestimmte Anweisungen des Verantwortlichen, einschließlich der Unterstützung des Auftragsverarbeiters bei Audits, Inspektionen, Datenschutz-Folgenabschätzungen oder der Bereitstellung jeglicher Unterstützung gemäß diesem AV-Vertrag, zusätzliche Gebühren verursachen können. In einem solchen Fall informiert der Auftragsverarbeiter den Verantwortlichen im Voraus über seine Gebühren für die Bereitstellung solcher Unterstützung und ist berechtigt, dem Verantwortlichen seine angemessenen Kosten und Ausgaben in Rechnung zu stellen, es sei denn, es wurde schriftlich etwas anderes vereinbart.

---

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche erkennt an und stimmt zu, dass der Auftragsverarbeiter Unterauftragsverarbeiter im Zusammenhang mit der Bereitstellung der Services einsetzen kann.

6.2 Alle Unterauftragsverarbeiter, die personenbezogene Daten im Rahmen der Services für den Verantwortlichen verarbeiten, halten sich an die in diesem AV-Vertrag festgelegten Pflichten des Auftragsverarbeiters.

6.3 Der Verantwortliche ermächtigt den Auftragsverarbeiter, die in der Liste der Unterauftragsverarbeiter aufgeführten Unterauftragsverarbeiter (veröffentlicht unter: https://amnexis.com/de/quixxs-legals/) zur Verarbeitung personenbezogener Daten zu verwenden. Während der Laufzeit dieses AV-Vertrags wird der Auftragsverarbeiter den Verantwortlichen mindestens 30 Tage im Voraus per E-Mail über Änderungen an der Liste der Unterauftragsverarbeiter informieren, bevor ein neuer oder ersetzender Unterauftragsverarbeiter zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung der Services autorisiert wird.

6.4 Der Verantwortliche kann der Nutzung eines neuen oder ersetzenden Unterauftragsverarbeiter widersprechen, indem er den Auftragsverarbeiter innerhalb von fünfzehn (15) Tagen nach Erhalt der Mitteilung des Auftragsverarbeiters schriftlich informiert. Falls der Verantwortliche einem neuen oder ersetzenden Unterauftragsverarbeiter widerspricht, kann der Verantwortliche den Hauptvertrag in Bezug auf jene Services kündigen, die ohne den Einsatz des neuen oder ersetzenden Unterauftragsverarbeiter nicht erbracht werden können. Der Auftragsverarbeiter wird dem Verantwortlichen alle vorausbezahlten Gebühren erstatten, die den Rest der Laufzeit des Hauptvertrags für solche gekündigten Services betreffen.

6.5 Alle Unterauftragsverarbeiter, die personenbezogene Daten verarbeiten, halten sich an die in diesem AV-Vertrag festgelegten Pflichten des Auftragsverarbeiters. Der Auftragsverarbeiter wird, bevor der relevante Unterauftragsverarbeiter
(i) jeden Unterauftragsverarbeiter
(ii) sicherstellen, dass jeder Unterauftragsverarbeiter sämtliche dieser Pflichten einhält.

6.6 Der Verantwortliche stimmt zu, dass der Auftragsverarbeiter und seine Unterauftragsverarbeiter Eingeschränkte Übermittlungen personenbezogener Daten vornehmen dürfen, um die Services für den Verantwortlichen gemäß der Regelungen des Hauptvertrags bereitzustellen. Der Auftragsverarbeiter bestätigt, dass solche

Unterauftragsverarbeiter:
(i) sich in einem Drittland oder Gebiet befinden, das von der EU-Kommission oder einer Aufsichtsbehörde als angemessen geschützt anerkannt wurde; oder
(ii) die geltenden Standardvertragsklauseln (SCCs) mit dem Auftragsverarbeiter abgeschlossen haben; oder
(iii) andere rechtlich anerkannte geeignete Garantien eingerichtet haben.

---

7. Eingeschränkte Übermittlungen

7.1 Die Parteien vereinbaren, dass bei einer Übermittlung personenbezogener Daten zwischen dem Verantwortlichen und dem Auftragsverarbeiter oder vom Auftragsverarbeiter an einen Unterauftragsverarbeiter, die eine Eingeschränkte Übermittlung darstellt, die anwendbaren SCCs gelten.

7.2 Für Eingeschränkte Übermittlungen aus dem EWR gelten die EU-SCCs. Diese werden als Teil dieses AV-Vertrags abgeschlossen und wie folgt ausgefüllt:
(i) Modul Zwei (Verantwortlicher an Auftragsverarbeiter) gilt, wenn der Kunde im Hinbllick auf die personenbezogenen Daten Verantwortlicher ist und das Unternehmen die Daten in seinem Auftrag verarbeitet;
(ii) Modul Drei (Auftragsverarbeiter an Auftragsverarbeiter) gilt, wenn das Unternehmen als Auftragsverarbeiter handelt und Unterauftragsverarbeiter einsetzt;
(iii) Modul Vier (Auftragsverarbeiter an Verantwortlicher) gilt, wenn das Unternehmen personenbezogene Daten verarbeitet und der Kunde nicht der EU- oder UK-DSGVO unterliegt;
(iv) In Klausel 7 der EU-SCCs gilt die optionale Docking-Klausel nicht;
(v) In Klausel 9 der EU-SCCs gilt Option 2, und die Frist für die Benachrichtigung über Änderungen von Unterauftragsverarbeitern ist in Klausel 6.3 dieses AV-Vertrags festgelegt;
(vi) In Klausel 11 der EU-SCCs gilt die optionale Sprache nicht;
(vii) In Klausel 17 der EU-SCCs gilt Option 1, und die EU-SCCs unterliegen irischem Recht;
(viii) In Klausel 18(b) der EU-SCCs werden Streitigkeiten vor den irischen Gerichten beigelegt;
(ix) Anhang I der EU-SCCs wird mit den Angaben in Anhang A dieses AV-Vertrags ausgefüllt;
(x) Anhang II der EU-SCCs wird mit den Angaben in Anhang B dieses AV-Vertrags ausgefüllt.

7.3 Anpassungen der EU-SCCs bei Anwendung des FADP:
(i) Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist die einzige Aufsichtsbehörde für Übermittlungen ausschließlich gemäß FADP;
(ii) Übermittlungen, die sowohl dem FADP als auch der EU-DSGVO unterliegen, werden von der in Anhang A dieses AV-Vertrags genannten EU-Aufsichtsbehörde bearbeitet;
(iii) Der Begriff "Mitgliedstaat" wird so ausgelegt, dass er die Rechte von betroffenen Personen in der Schweiz nicht ausschließt;
(iv) Bei Übermittlungen, die ausschließlich dem FADP unterliegen, sind Verweise auf die DSGVO als Verweise auf das FADP zu verstehen;
(v) Bei Übermittlungen, die sowohl dem FADP als auch der EU-DSGVO unterliegen, gelten

Verweise auf die EU-DSGVO insoweit als Verweise auf das FADP, wie die Übermittlungen dem FADP unterliegen.

7.4 Für Eingeschränkte Übermittlungen aus dem Vereinigten Königreich gelten die UK-SCCs. Diese werden als Teil dieses AV-Vertrags abgeschlossen und wie folgt ausgefüllt:
(i) Tabelle 1 der UK-SCCs wird mit den Angaben in Anhang A dieses AV-Vertrags ausgefüllt;
(ii) Tabelle 2 der UK-SCCs wird mit den Angaben in Klauseln 7.2(i)-(viii) dieses AV-Vertrags ausgefüllt;
(iii) Tabelle 3 der UK-SCCs wird mit den Angaben in den Anhängen A und B dieses AV-Vertrags ausgefüllt;
(iv) Jede Partei kann die UK-SCCs gemäß Klausel 19 der UK-SCCs kündigen.

7.5 Sollten die EU-SCCs oder UK-SCCs zukünftig geändert werden, vereinbaren die Parteien, die notwendigen Anpassungen nach Treu und Glauben zu verhandeln, um die Einhaltung des geltenden Datenrechts sicherzustellen.

7.6 Im Falle von Widersprüchen zwischen diesem AV-Vertrag und den anwendbaren SCCs haben die Bestimmungen der SCCs Vorrang.

7.7 Sollten Länder außerhalb des EWR, des Vereinigten Königreichs oder der Schweiz ähnliche Vorschriften wie die SCCs einführen, verpflichten sich die Parteien, diese Klauseln bei Bedarf abzuschließen.

---

8. Betroffenenanfragen

8.1 Der Verantwortliche kann die Berichtigung, Löschung, Sperrung und/oder Bereitstellung personenbezogener Daten während oder nach Beendigung des Hauptvertrags verlangen. Der Verantwortliche erkennt an, dass der Auftragsverarbeiter solche Anfragen nach geltendem Recht verarbeitet und in Übereinstimmung mit seinen internen Prozessen erfüllt.

8.2 Erhält der Auftragsverarbeiter eine Anfrage von einem Betroffenen, leitet er diese Anfrage an den Verantwortlichen weiter, sofern dies nicht gesetzlich untersagt ist. Der Verantwortliche erstattet dem Auftragsverarbeiter die entstandenen Kosten für die Unterstützung bei der Bearbeitung solcher Anfragen. Muss der Auftragsverarbeiter gesetzlich auf eine Anfrage reagieren, wird der Verantwortliche in vollem Umfang kooperieren.

---

9. Audits

9.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die vernünftigerweise erforderlich sind, um die Einhaltung der Verarbeitungspflichten nachzuweisen, und ermöglicht Audits und Inspektionen.

9.2 Audits basieren auf den neuesten Berichten, Zertifikaten oder Auszügen eines unabhängigen, zur Vertraulichkeit verpflichteten Prüfers. Reicht dies nicht aus, kann der Verantwortliche eine umfangreichere Prüfung durchführen, die:

(i) auf Kosten des Verantwortlichen erfolgt;
(ii) im Umfang auf vereinbarte Themen beschränkt ist;
(iii) während der Geschäftszeiten des Auftragsverarbeiters und mit einer Frist von mindestens vier Wochen durchgeführt wird, es sei denn, ein schwerwiegendes Problem liegt vor; und
(iv) den Geschäftsbetrieb des Auftragsverarbeiters nicht beeinträchtigt.

9.3 Diese Klausel soll die Prüfungsrechte des Verantwortlichen klären, ohne sie einzuschränken.

---

10. Verletzung des Schutzes personenbezogener Daten

10.1 Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich benachrichtigen, nachdem er Kenntnis (und in jedem Fall innerhalb von 72 Stunden nach Entdeckung) von
10.2 Im Falle einer Verletzung des Schutzes personenbezogener Daten wird der Auftragsverarbeiter alle wirtschaftlich zumutbaren Maßnahmen ergreifen, um die personenbezogenen Daten zu sichern, die Auswirkungen der Verletzung zu begrenzen und den Verantwortlichen bei der Erfüllung seiner aus anwendbarem Recht folgenden Pflichten unterstützen.

11. Compliance, Kooperation und Kommunikation

11.1 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über jede Anfrage oder Beschwerde bezüglich der Verarbeitung personenbezogener Daten benachrichtigen, die den Verantwortlichen nachteilig betrifft, es sei denn, eine solche Benachrichtigung ist nach geltendem Recht oder einer relevanten gerichtlichen Anordnung nicht zulässig.
11.2 Der Auftragsverarbeiter kann Kopien von personenbezogenen Daten anfertigen und/oder diese gemäß rechtlichen oder regulatorischen Anforderungen (einschließlich, aber nicht beschränkt auf Aufbewahrungspflichten) aufbewahren.
11.3 Der Auftragsverarbeiter wird den Verantwortlichen angemessen bei der Durchführung von Datenschutz-Folgenabschätzungen (DPIA) unterstützen, wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt werden.
11.4 Der Verantwortliche wird den Auftragsverarbeiter innerhalb eines angemessenen Zeitrahmens über Änderungen der geltenden Datenschutzgesetze, -vorschriften oder -richtlinien informieren, die die vertraglichen Pflichten des Auftragsverarbeiters betreffen könnten. Der Auftragsverarbeiter wird innerhalb eines angemessenen Zeitrahmens auf Änderungen reagieren, die an den Bedingungen dieses AV-Vertrags oder an den technischen und organisatorischen Maßnahmen zur Aufrechterhaltung der Compliance mit diesen vorgenommen werden müssen. Kann der Auftragsverarbeiter erforderliche Änderungen nicht umsetzen, kann der Verantwortliche den Teil oder die Teile der Services kündigen, die zur Nicht-Compliance führen. Soweit andere Teile der bereitgestellten Services nicht von solchen Änderungen betroffen sind, bleiben diese Services weiterhin unberührt.
11.5 Der Verantwortliche und der Auftragsverarbeiter sowie, soweit zutreffend, deren Vertreter werden auf Anfrage mit einer Aufsichtsbehörde bei der Erfüllung ihrer jeweiligen Pflichten gemäß diesem AV-Vertrag und dem Datenschutzrecht zusammenarbeiten.

12. Haftung

12.1 Die Haftungsbeschränkungen, die im Hauptvertrag festgelegt sind, gelten für alle Ansprüche, die aufgrund eines Verstoßes gegen die Bestimmungen dieses AV-Vertrags geltend gemacht werden.
12.2 Die Parteien vereinbaren, dass der Auftragsverarbeiter für Verstöße gegen die Bestimmungen dieses AV-Vertrags, die durch (fahrlässige) Handlungen und Unterlassungen seiner Unterauftragsverarbeiter verursacht werden, in demselben Umfang haftet, als wenn der Auftragsverarbeiter die Services jedes Unterauftragsverarbeiters direkt unter den Bedingungen des AV-Vertrags selbst erbringen würde, vorbehaltlich etwaiger Haftungsbeschränkungen, die in den Bestimmungen des Hauptvertrags festgelegt sind.
12.3 Die Parteien vereinbaren, dass der Verantwortliche für Verstöße gegen diesen AV-Vertrag, die durch (fahrlässige) Handlungen und Unterlassungen seiner verbundenen Unternehmen verursacht werden, haftet, als wenn solche Handlungen oder Unterlassungen vom Verantwortlichen selbst begangen worden wären.
12.4 Der Verantwortliche ist nicht berechtigt, mehr als einmal für denselben Schaden Schadenersatz zu verlangen.

13. Laufzeit und Beendigung

13.1 Der Auftragsverarbeiter darf personenbezogene Daten nur für die Dauer des AV-Vertrags verarbeiten. Die Laufzeit dieses AV-Vertrags beginnt mit dem Inkrafttreten des Hauptvertrages und endet automatisch mit der Kündigung oder dem Ablauf des Hauptvertrages.

14. Löschung und Rückgabe personenbezogener Daten

14.1 Der Auftragsverarbeiter wird nach Wahl des Verantwortlichen auf dessen schriftliche Anfrage hin, die innerhalb von 30 Tagen nach Beendigung der Bereitstellung der Services eingehen muss, personenbezogene Daten an den Verantwortlichen zurückgeben oder löschen. Der Auftragsverarbeiter wird in jedem Fall alle Kopien personenbezogener Daten in seinen Systemen innerhalb von einem Jahr nach wirksamer der Beendigung des Hauptvertrages oder der Deaktivierung des Kontos des Verantwortlichen löschen, es sei denn, anwendbares Recht verpflichtet ihn zur Aufbewahrung der personenbezogenen Daten über diesen Zeitraum hinaus.

15. Allgemeines

15.1 Dieser AV-Vertrag regelt das gesamte Verhältnis der Parteien in Bezug auf den hier behandelten Gegenstand abschließend.
15.2 Sollte eine Bestimmung dieses AV-Vertrags ungültig oder unwirksam werden, bleibt die rechtliche Wirkung der anderen Bestimmungen unberührt. Eine gültige Bestimmung, die dem wirtschaftlichen Ziel der Parteien am nächsten kommt, gilt als vereinbart und ersetzt die ungültige Bestimmung. Dasselbe gilt für etwaige Auslassungen.
15.3 Vorbehaltlich etwaiger Bestimmungen der SCCs, die entgegenstehen, unterliegt dieser AV-Vertrag deutschem Recht. Die Gerichte in Berlin haben die ausschließliche Zuständigkeit für die Beilegung aller Streitigkeiten, die sich aus diesem AV-Vertrag ergeben.

15.4 Die Parteien vereinbaren, dass dieser AV-Vertrag in die Bestimmungen des Hauptvertrages aufgenommen und durch diese geregelt wird.

Anhang A

Liste der Parteien, Beschreibung der Verarbeitung und Übermittlung personenbezogener Daten, zuständige Aufsichtsbehörde

A. LISTE DER PARTIEN

Datenexporteur

Bezeichnet den Kunden.

Adresse	Wie im Hauptvertrag für den Kunden angegeben.
Name, Position und Kontaktdaten der Kontaktperson	Wie vom Kunden in seinem Konto angegeben und für Benachrichtigungs- und Rechnungszwecke verwendet.
Aktivitäten, die für die über die SCCs übertragenen Daten relevant sind	Nutzung der Services.
Unterschrift und Datum	Durch den Abschluss des Hauptvertrages gilt der Datenexporteur als Unterzeichner der in diesen AV-Vertrags aufgenommenen SCCs einschließlich ihrer Anhänge, ab dem Wirksamkeitsdatum des Hauptvertrages.
Rolle	Verantwortlicher.
Name des Vertreters (falls zutreffend)	Jeder UK- oder EU-Vertreter, der in der Datenschutzerklärung des Datenexporteurs benannt ist.

Datenimporteur

Bezeichnet Amnexis Holding Ltd, handelnd unter dem Namen QUIXXS.	
Adresse	Guinness Enterprise Centre Taylor's Lane - Dublin D08 YE0P IRELAND
Name, Position und Kontaktdaten der Kontaktperson	

Aktivitäten, die für die über die SCCs übertragenen Daten relevant sind	Bereitstellung von Cloud-Computing-Lösungen für den Datenexporteur, bei denen der Datenimporteur personenbezogene Daten gemäß den Anweisungen des Datenexporteurs im Einklang mit den Bestimmungen des Hauptvertrages verarbeitet.
Unterschrift und Datum	Durch den Abschluss des Vertrages gilt der Datenimporteur als Unterzeichner der in diesen AV-Vertrags aufgenommenen SCCs einschließlich ihrer Anhänge, ab dem Wirksamkeitsdatum des Hauptvertrages.
Rolle	Auftragsverarbeiter.

B. BESCHREIBUNG DER VERARBEITUNG UND ÜBERMITTLUNG

Kategorien von betroffenen Personen	Mitarbeiter, Vertreter, Berater, Consultants und freiberuflich für den Verantwortlichen tätige Personen (die natürliche Personen sind), die von Patienten für medizinische Behandlungen, Gesundheitsdienstleistungen oder Pflegeleistungen konsultiert werden. Patienten der oben genannten Personen.
Kategorien personenbezogener Daten	Der Verantwortliche kann personenbezogene Daten an die Services übermitteln, deren Umfang vom Verantwortlichen bestimmt und kontrolliert wird. Zu den personenbezogenen Daten gehören unter anderem: ● Persönliche Angaben wie Vorname, Nachname, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Familienstand und Geschlecht der Patienten und autorisierten Nutzer. ● Individuelle Kennungen wie Benutzername, Kontonummer oder Passwort der Nutzer. ● Audio- und Videoaufzeichnungen von Patientenberatungen und medizinischen Daten. ● Personenbezogene Daten in E-Mail- und Nachrichteninhalten, die zur Identifikation einer Person verwendet werden können oder diese identifizieren. ● Metadaten, einschließlich „gesendet“, „an“, „von“, „Datum“, „Uhrzeit“, „Betreff“, die personenbezogene Daten enthalten können. ● Geolocation basierend auf der IP-Adresse. ● Medizinische Daten und Patientenakten.

B. BESCHREIBUNG DER VERARBEITUNG UND ÜBERMITTLUNG

	● Daten zu Ausbildung und Beruf. ● Dateianhänge, die personenbezogene Daten enthalten können. ● Umfragen, Feedback- und Bewertungsnachrichten. ● Informationen, die von Nutzern der Services im Rahmen von Supportanfragen bereitgestellt werden. ● Andere Daten, die vom Verantwortlichen von Zeit zu Zeit hinzugefügt werden.
Sensible Daten	Die übertragenen personenbezogenen Daten umfassen, sind jedoch nicht beschränkt auf, folgende besondere Kategorien personenbezogener Daten: ● Daten, die die rassische oder ethnische Herkunft offenbaren. ● Religiöse oder philosophische Überzeugungen. ● Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
Häufigkeit der Verarbeitung und Übermittlung	Kontinuierlich während der Laufzeit des Hauptvertrages.
Art der Verarbeitung	Verarbeitungsprozesse umfassen unter anderem: ● Audio- und Videoaufzeichnungen von Gesprächen zwischen Ärzten oder anderen Personen, die medizinische Behandlungen, Gesundheitsdienstleistungen oder Pflegeleistungen erbringen und Patienten in verschiedenen (vom Benutzer ausgewählten) Formaten in Echtzeit zu erstellen, nämlich als Zusammenfassungsberichte, einschließlich automatischer Formular-Ausfüllungen für Erhebungsbögen, medizinische Berichte, Vitaldaten und Überweisungsbriefe. ● Übersetzung aller mündlichen Informationen in die bevorzugte Sprache des Nutzers in schriftlicher Form.
Zweck(e) der Datenübermittlung und der weiteren Verarbeitung	Personenbezogene Daten werden an Unterauftragsverarbeiter übertragen, die einen Teil der personenbezogenen Daten verarbeiten müssen, um ihre Leistungen (im Rahmen der Services, die der Auftragsverarbeiter dem Verantwortlichen bereitstellt) zu erbringen.
Zeitraum der Aufbewahrung personenbezogener Daten	Sofern nicht anders schriftlich vereinbart, für die Dauer des Hauptvertrages, vorbehaltlich der Klausel 14 des AV-Vertrags.

B. BESCHREIBUNG DER VERARBEITUNG UND ÜBERMITTLUNG

Für Übermittlungen an (Unter-)Auftragsverarbeiter auch den Gegenstand, die Art und die Dauer der Verarbeitung angeben	Die Unterauftragsverarbeiter-Liste, die unter dem folgenden Link veröffentlicht ist: https://amnexis.com/de/quixxs-legals/ gibt die von jedem Unterauftragsverarbeiter verarbeiteten personenbezogenen Daten sowie die von jedem Unterauftragsverarbeiter erbrachten Leistungen an.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Identifizieren Sie die zuständige(n) Aufsichtsbehörde(n) (z. B. gemäß Klausel 13 der Standardvertragsklauseln):

Anwendbares Gesetz	Zuständige Aufsichtsbehörde
EU-DSGVO	Irische Datenschutzbehörde - Data Protection Commission (DPC)
UK-DSGVO	Information Commissioner's Office (ICO) im Vereinigten Königreich
Schweizerisches Datenschutzgesetz (FADP)	Schweizerischer Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (FDPIC)

Anhang B

Technische und organisatorische Sicherheitsmaßnahmen
(Einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit)

Nachfolgend wird eine Beschreibung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters (einschließlich relevanter Zertifizierungen) zur Gewährleistung eines angemessenen Sicherheitsniveaus gegeben, unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.
Soweit zutreffend, dient dieser Anhang B als Anhang II zu den Standardvertragsklauseln (SCCs).

Maßnahme	Beschreibung
Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten	Verschlüsselungstechnologie wird zur Übertragungssteuerung verwendet (z. B. VPN-Tunnel und vollständige Festplattenverschlüsselung). Ein individueller Verschlüsselungsschlüssel wird für den Verantwortlichen unter Verwendung einer FIPS 140-2-konformen Krypto-Bibliothek generiert. Archivierte Daten werden mit AES256-Bit-Verschlüsselung verschlüsselt, und Daten im Transit sind durch Transport Layer Security (TLS) geschützt.
Maßnahmen zur Gewährleistung der fortlaufenden Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz der Verarbeitungssysteme und -dienste	Der Zugriff auf notwendige Daten wird durch ein entsprechendes Rollen- und Berechtigungskonzept innerhalb der Systeme und Anwendungen sichergestellt. Im Einklang mit den Prinzipien der „minimalen Rechte“ und des „Need-to-Know“ hat jede Rolle nur die für die Erfüllung der Aufgabe erforderlichen Rechte.
Maßnahmen zur Gewährleistung der Wiederherstellbarkeit der Verfügbarkeit und des Zugriffs auf personenbezogene Daten in angemessener Zeit im Falle eines physischen oder technischen Vorfalls	Daten werden in Triplikaten in 2 Rechenzentren mit Kreuzverbindungen gespeichert. Redundanz wird aufrechterhalten, und Daten werden stündlich und täglich gesichert. Eine Notfallwiederherstellungsstrategie ist vorhanden und wird jährlich geübt. Es werden interne Audits durchgeführt, und ein Großteil der Infrastrukturüberwachung ist

Maßnahme	Beschreibung
Prozesse zur regelmäßigen Überprüfung, Bewertung und Auswertung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	automatisiert. Ein externes Sicherheits- und Compliance-Audit wird jährlich durchgeführt.
Maßnahmen zur Benutzeridentifikation und -autorisierung	Remote-Zugriff auf die Datenverarbeitungssysteme ist nur über den sicheren VPN-Tunnel des Auftragsverarbeiters möglich. Nach erfolgreicher Authentifizierung wird die Autorisierung durch die Bereitstellung eines individuellen Benutzernamens und Passworts für einen zentralen Verzeichnisdienst ausgeführt.
Maßnahmen zum Schutz von Daten während der Übermittlung	Alle Zugriffsversuche, sowohl erfolgreich als auch erfolglos, werden protokolliert und überwacht. Daten im Transit sind durch Transport Layer Security (TLS) geschützt.
Maßnahmen zum Schutz von Daten während der Speicherung	Personenbezogene Daten werden nur intern und auf den Servern von Drittanbieter-Rechenzentren gespeichert, die ISO 7001 und 270018-Zertifizierungen besitzen. Archivierte Daten des Verantwortlichen sind mit AES256-Verschlüsselung im Ruhezustand und TLS während der Übertragung geschützt.
Maßnahmen zur Gewährleistung der physischen Sicherheit der Standorte, an denen personenbezogene Daten verarbeitet werden	Geschäftsgebäude sind aufgrund ihrer jeweiligen Sicherheitsanforderungen in verschiedene Sicherheitszonen unterteilt, die unterschiedliche Zugriffsberechtigungen haben. Rechenzentren von Drittanbietern werden durch Sicherheitspersonal überwacht. Der Zugang für Mitarbeiter ist nur mit einem ID-Ausweis möglich, der ein Foto enthält. Alle anderen Personen haben nur nach vorheriger Anmeldung Zugang (z. B. am Haupteingang).
Maßnahmen zur Gewährleistung der Ereignisprotokollierung	Systemeingaben werden in Form von Protokolldateien aufgezeichnet, sodass im Nachhinein überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, geändert oder gelöscht wurden.
Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	Unsere Systemkonfiguration basiert auf den Sicherheits-Technical Implementation Guides (STIG). Die Systemkonfiguration wird durch Softwaretools angewendet und gepflegt, die

Maßnahme	Beschreibung
	sicherstellen, dass die Systemkonfigurationen nicht von den Spezifikationen abweichen. Abweichungen werden automatisch behoben und unserem SOC gemeldet.
Maßnahmen für interne IT- und IT-Sicherheitsgovernance und -management	Mitarbeiter werden angewiesen, personenbezogene Daten nur im Rahmen und zu den Zwecken ihrer Aufgaben (z. B. Servicebereitstellung) zu erheben, zu verarbeiten und zu nutzen. Auf technischer Ebene umfasst die Multi-Client-Fähigkeit eine Trennung der Funktionen sowie eine geeignete Trennung von Test- und Produktionssystemen.
Maßnahmen zur Zertifizierung/Sicherung von Prozessen und Produkten	Die technischen und organisatorischen Maßnahmen basieren auf den internationalen Normen ISO 27001 und ISO 27018. Der Auftragsverarbeiter verwendet Rechenzentren von Drittanbietern, die diese Zertifizierungen aufrechterhalten, und stellt dem Verantwortlichen auf schriftliche Anfrage jährlich einen Bericht über die neuesten Zertifizierungs- und/oder Bestätigungsberichte zur Verfügung.
Maßnahmen zur Gewährleistung der Datenminimierung	Personenbezogene Daten werden umgehend gelöscht, wenn sie nicht mehr für die Zwecke benötigt werden, für die sie verarbeitet wurden. Bei jeder Löschung werden die personenbezogenen Daten zunächst gesperrt und dann mit einer gewissen Verzögerung endgültig gelöscht, um versehentliche Löschungen oder mögliche absichtliche Schäden zu verhindern.
Maßnahmen zur Gewährleistung der Datenqualität	Alle Daten, die der Auftragsverarbeiter besitzt, werden vom Verantwortlichen bereitgestellt. Der Auftragsverarbeiter bewertet die Qualität der vom Verantwortlichen bereitgestellten Daten nicht. Der Auftragsverarbeiter stellt im Rahmen des Produkts Reporting-Tools zur Verfügung, mit denen der Verantwortliche die gespeicherten Daten verstehen und validieren kann.
Maßnahmen zur Gewährleistung der begrenzten Datenspeicherung	Der Auftragsverarbeiter verwendet ein Datenklassifizierungssystem für alle Daten, die er speichert, und unsere Aufbewahrungsrichtlinie legt fest, wie lange jede Art von Daten aufbewahrt wird. Wenn ein Datensatz mit personenbezogenen Daten gelöscht wird, wird er dauerhaft aus unseren aktiven Datenbanken entfernt. Daten werden in unseren Backups aufbewahrt, bis sie gemäß der

Maßnahme	Beschreibung
	Aufbewahrungsrichtlinie durch neuere Backups ersetzt werden.
Maßnahmen zur Gewährleistung der Rechenschaftspflicht	Der Auftragsverarbeiter überprüft seine Informationssicherheitsrichtlinie halbjährlich, um sicherzustellen, dass sie weiterhin relevant ist und befolgt wird. Alle Mitarbeiter, die mit sensiblen Daten arbeiten, müssen die Informationssicherheitsrichtlinie anerkennen und werden jährlich zu dieser geschult. Es gibt eine Disziplinarrichtlinie für Mitarbeiter, die sich nicht an die Informationssicherheitsrichtlinie halten.
Maßnahmen zur Ermöglichung der Datenportabilität und Gewährleistung der Löschung	Die Services verfügen über integrierte Tools, die es dem Verantwortlichen ermöglichen, Daten zu exportieren und dauerhaft zu löschen.
Maßnahmen, die vom (Unter) Auftragsverarbeiter ergriffen werden, um dem Verantwortlichen Unterstützung zu bieten	Die Übermittlung personenbezogener Daten an Dritte (z. B. Kunden, Unterauftragsverarbeiter, Dienstleister) erfolgt nur, wenn ein entsprechender Vertrag besteht und nur zu den spezifischen Zwecken. Wenn personenbezogene Daten außerhalb des EWR übertragen werden, stellt der Auftragsverarbeiter sicher, dass ein angemessenes Datenschutzniveau an dem Zielort oder der Organisation gemäß den Datenschutzanforderungen der Europäischen Union besteht, z. B. durch den Einsatz von Verträgen basierend auf den EU-SCCs.