Anlage zur Datenverarbeitung (Verantwortlicher – Auftragsverarbeiter)

Diese Anlage zur Datenverarbeitung, einschließlich der Datenverarbeitungsbedingungen und der Beschreibung der Kontrollen des Auftragsverarbeiters (diese „DPA“), ist dem Vertrag zwischen dem Nutzer und GHX als dem für die Datenverarbeitung Verantwortlichen bzw. dem Auftragsverarbeiter beigefügt und wird Bestandteil des Vertrags. Die Parteien vereinbaren Folgendes:

1. Begriffsbestimmungen und Informationen zur Datenverarbeitung

Zusätzlich zu den oben und an anderer Stelle im Vertrag definierten Begriffen haben die hier verwendeten, hervorgehobenen Begriffe die nachstehend angegebene Bedeutung. Hervorgehobene Begriffe, die in dieser DPA oder im Vertrag verwendet werden, aber nicht anderweitig definiert sind, haben die Bedeutung, die ihnen in der DSGVO (wie unten definiert) zugewiesen wird.

Definierter Begriff	Begriffsbestimmung
Datenkategorien	Kontaktdaten; Beschäftigungsdaten; Gesundheitsdaten; Informationen über IT-Systeme; E-Mail-Inhalte und übermittelte Daten; Informationen über angebotene Waren und Dienstleistungen; Finanzdaten.
Betroffenen Personen	• Ehemalige, gegenwärtige und künftige Mitarbeiter, Auftragnehmer, Lieferanten und Vertreter des Verantwortlichen; • Ehemalige, gegenwärtige und zukünftige Patienten des Verantwortlichen sowie deren Eltern, Vormünder und Begünstigte.
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016; oder 1. für Nutzer mit Sitz im Vereinigten Königreich (das „Vereinigte Königreich“) das britische Datenschutzgesetz („Data Protection Act 2018“) und die DSGVO, wie sie gemäß Abschnitt 3 des Gesetzes über den Austritt aus der Europäischen Union („European Union (Withdrawal) Act 2018“) und in der durch die Verordnung über den Datenschutz, den Schutz der Privatsphäre und die elektronische Kommunikation („Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019“) geänderten Fassung Teil des Rechts von England, Wales, Schottland und Nordirland sind; oder 2. für Nutzer mit Sitz in der Schweiz die Neufassung des Bundesgesetzes über den Datenschutz und seine Ausführungsverordnungen, die am 1. September 2023 in Kraft getreten sind (revDSG)
Personen-bezogene Daten	Gemäß der Definition in der DSGVO, insbesondere personenbezogene Daten, die vom Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet werden.
Art der Datenverar beitung	Jeder mit oder ohne Hilfe von Mitteln oder Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten, insbesondere das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten.
Verarbeitungs-standorte	• Büros des Verantwortlichen in Cambridge, Vereinigtes Königreich; Brüssel, Belgien; Düsseldorf, Frankfurt, Königstein im Taunus, und Koblenz, Deutschland; Hilversum, Niederlande; Baar, Schweiz, und Colorado, Vereinigte Staaten von Amerika; • Rechenzentren des Verantwortlichen bei Anbietern in der EU/im EWR, im Vereinigten Königreich, in Norwegen, in Kanada, in Texas, Virginia und Washington in den Vereinigten Staaten von Amerika und in Indien

Zweck der Datenverarbeitung	• Die berechtigten Interessen des Verantwortlichen, seiner Lieferanten, Auftragnehmer und Vertreter oder des Auftragsverarbeiters bei der Vertragserfüllung. • Präventiv- oder Arbeitsmedizin, zur Beurteilung der Arbeitsfähigkeit der betroffenen Person, medizinische Diagnose, die Bereitstellung von Gesundheits- oder Sozialleistungen oder Behandlungen oder die Verwaltung von Gesundheits- oder Sozialsystemen und -diensten auf der Grundlage des Rechts der Europäischen Union oder der Mitgliedstaaten oder aufgrund eines Vertrags mit einem Angehörigen der Gesundheitsberufe und vorbehaltlich der Bedingungen und Garantien in der DSGVO in Bezug auf die Verarbeitung unter der Verantwortung eines Angehörigen der Gesundheitsberufe, der nach dem Recht der Europäischen Union oder der Mitgliedstaaten oder den von den zuständigen nationalen Stellen erlassenen Vorschriften dem Berufsgeheimnis unterliegt, oder durch eine andere Person, die nach dem Recht der Europäischen Union oder der Mitgliedstaaten oder den von den zuständigen nationalen Stellen erlassenen Vorschriften ebenfalls dem Berufsgeheimnis unterliegt.

Definierter Begriff	Begriffsbestimmung
DPA	Diese Anlage zur Datenverarbeitung, bestehend aus diesem Deckblatt und den folgenden Anhängen: 1. die Geschäftsbedingungen für die Datenverarbeitung; und 2. die Beschreibung der Kontrollen des Auftragsverarbeiters.
Controller	Der Nutzer, zusammen mit seinen verbundenen Unternehmen und lizenzierten Einrichtungen, wie im Vertrag angegeben.
Auftragsver-arbeiter	Die im Vertrag genannte Entität von GHX.
Vertrag	Der Vertrag/die Verträge über Dienste zwischen den Parteien oder den mit ihnen verbundenen Unternehmen, einschließlich aller Nachträge, Anlagen, Anhänge, Änderungen und Service-Aufträgen.

Geschäftsbedingungen für die Datenverarbeitung

2. Aufnahme in den Vertrag

Die Parteien vereinbaren, dass dieser DPA mit dem Datum des Inkrafttretens des Vertrags (das „Datum des Inkrafttretens“) in den Vertrag aufgenommen wird.

3. Datenverarbeitung

a. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen und in Übereinstimmung mit dem Vertrag, auch im Hinblick auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, es sei denn, das Recht der Europäischen Union oder nationales Recht, dem der Auftragsverarbeiter unterliegt, schreibt etwas anderes vor; in diesem Fall unterrichtet der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über dieses rechtliche Erfordernis, es sei denn, dieses Recht verbietet eine solche Unterrichtung aus wichtigen Gründen des öffentlichen Interesses.

b. Der Vertrag und dieser DPA stellen die allgemeinen schriftlichen Anweisungen des Verantwortlichen für die Verarbeitung personenbezogener Daten dar, mit der Maßgabe, dass der Verantwortliche für die Verarbeitung personenbezogener Daten spezifische Anweisungen erteilen kann, die diese Verarbeitung weiter einschränken, sofern dies im Einklang mit dem anwendbaren Recht steht.

c. Der Auftragsverarbeiter darf die personenbezogenen Daten nicht ohne vorherige Prüfung und schriftliche Zustimmung des Verantwortlichen für andere Zwecke als auf dem Deckblatt dieser DPA genannten Zwecke verarbeiten.

d. Jede Berichtigung, Einschränkung der Verarbeitung und Löschung personenbezogener Daten darf nur auf Anweisung des Verantwortlichen erfolgen.

e. Wenn der Auftragsverarbeiter aufgrund der Festlegung der Zwecke und Mittel der Verarbeitung personenbezogener Daten ein gemeinsamer Verantwortlicher im Sinne der DSGVO in Bezug auf diese personenbezogenen Daten ist, muss der Auftragsverarbeiter die Bestimmungen des anwendbaren Rechts in Bezug auf die Verantwortlichen im Hinblick auf diese personenbezogenen Daten einhalten. Unter diesen Umständen bleibt der Verantwortliche die Kontaktstelle für die betroffenen Personen.

f. Die Parteien halten sich bei der Ausführung dieser DPA und des Vertrages an geltendes Recht, insbesondere an die DSGVO.

g. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass eine Weisung des Verantwortlichen gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

4. Vertraulichkeit

a. Der Auftragsverarbeiter ist verpflichtet, personenbezogene Daten in Übereinstimmung mit dem anwendbaren Recht und dem Vertrag vertraulich zu behandeln und dabei nicht weniger als wirtschaftlich angemessene Kontrollen anzuwenden.

b. Der Auftragsverarbeiter stellt sicher, dass die Personen, denen er die Verarbeitung personenbezogener Daten gestattet, sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen.

c. Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche und/oder seine Kommunikationspartner beim Austausch von genetischen Daten, biometrischen Daten oder Gesundheitsdaten über die Dienste des Auftragsverarbeiters nach dem Recht der Union oder der Mitgliedstaaten zur Vertraulichkeit verpflichtet sind, und er erkennt an und erklärt sich damit einverstanden, dass er bei der Verarbeitung solcher Daten ebenfalls einer solchen Verpflichtung unterliegt.

5. Sicherheit

a. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ergreift der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen,

um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, einschließlich u. a:

i. die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten;

ii. die Fähigkeit, die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste zu gewährleisten;

iii. die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls schnell wiederherzustellen; und

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

b. Bei der Beurteilung des angemessenen Sicherheitsniveaus berücksichtigt der Auftragsverarbeiter insbesondere die Risiken im Zusammenhang mit der Verarbeitung, einschließlich der unbeabsichtigten oder unrechtmäßigen Vernichtung, des Verlusts, der Veränderung, der unberechtigten Weitergabe oder des unberechtigten Zugriffs auf die übermittelten, gespeicherten oder auf andere Weise verarbeiteten personenbezogenen Daten.

c. Der Auftragsverarbeiter kann seine dokumentierte Einhaltung eines genehmigten Verhaltenskodex gemäß Artikel 40 DSGVO (oder einer nach geltendem Recht gleichwertigen Bestimmung) oder eines genehmigten Zertifizierungsmechanismus gemäß Artikel 42 DSGVO (oder einer nach geltendem Recht gleichwertigen Bestimmung) als ein Element zum Nachweis der Einhaltung der Anforderungen an technische und organisatorische Maßnahmen gemäß dieser DPA verwenden. In diesen Fällen stellt der Auftragsverarbeiter dem Verantwortlichen eine aktualisierte Dokumentation zur Verfügung, aus der hervorgeht, dass die Bestimmungen eingehalten werden, und bringt diese Dokumentation unverzüglich auf den neuesten Stand, wenn sich die Umstände in Bezug auf den Auftragsverarbeiter wesentlich ändern.

d. Der Auftragsverarbeiter ergreift Maßnahmen, um sicherzustellen, dass jede natürliche Person, die für den Auftragsverarbeiter tätig ist und Zugang zu personenbezogenen Daten hat, diese nur auf Weisung des Verantwortlichen verarbeitet, es sei denn, es bestehen Verpflichtungen aufgrund des Rechts der Europäischen Union oder eines Mitgliedstaats.

e. Der Auftragsverarbeiter hat Maßnahmen ergriffen und umgesetzt, die geeignet sind, die Anforderungen der DSGVO, der anwendbaren nationalen und anderer Datenschutzgesetze, der Beschreibung der Kontrollen des Auftragsverarbeiters im Anhang zu dieser DPA und anderer anwendbarer Gesetze zu erfüllen. Der Auftragsverarbeiter muss dem Verantwortlichen auf schriftliche Anfrage jederzeit Kopien dieser Richtlinien zur Verfügung stellen.

6. Unterauftragsverarbeiter

a. Der Auftragsverarbeiter darf ohne vorherige ausdrückliche oder allgemeine schriftliche Zustimmung des Verantwortlichen keinen anderen Datenverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen. Die Parteien vereinbaren, dass alle Bestimmungen des Vertrags, die ausdrücklich die Beauftragung von Unterauftragnehmern gestatten, eine allgemeine schriftliche Zustimmung des Verantwortlichen zur Unterverarbeitung durch verbundene Unternehmen des Auftragsverarbeiters und durch Unterauftragsverarbeiter, die Dienstleistungen in den Bereichen Business Process Outsourcing, Informationstechnologie, Datenhosting und -speicherung, Telekommunikation sowie Rechts- und Buchhaltungsdienstleistungen erbringen, darstellen. Der Auftragsverarbeiter informiert den Verantwortlichen auf dessen schriftliches Ersuchen hin nicht öfter als einmal pro Jahr über beabsichtigte Änderungen in Bezug auf die Einbeziehung oder Ersetzung anderer Auftragsverarbeiter, die regelmäßig Zugang zu mehr als geringfügigen Mengen personenbezogener Daten haben.

b. Beauftragt der Auftragsverarbeiter einen anderen Datenverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Verantwortlichen, so schließt der Auftragsverarbeiter mit diesem anderen Datenverarbeiter einen schriftlichen Vertrag, in dem mindestens das gleiche Maß an Datenschutzverpflichtungen festgelegt ist wie in dieser DPA, im Vertrag oder in einem anderen Rechtsakt zwischen dem Verantwortlichen und dem Auftragsverarbeiter, auf den in dieser DPA oder in der DSGVO Bezug genommen wird. Ein solcher Vertrag muss insbesondere hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so umgesetzt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser DPA, der DSGVO und/oder anderer anwendbarer Rechtsvorschriften erfolgt,

und, falls der andere Datenverarbeiter in einer Rechtsordnung niedergelassen ist, die kein angemessenes Datenschutzniveau gewährleistet, ein solches Datenschutzniveau sicherstellen (*z. B.* durch Standardvertragsklauseln). Der Verantwortliche ermächtigt den Auftragsverarbeiter, Standardvertragsklauseln mit Unterauftragsverarbeitern in den oben genannten Kategorien abzuschließen, die die Übermittlung personenbezogener Daten in die Länder abdecken, die im Deckblatt dieser DPA unter „Verarbeitungsstandorte“ aufgeführt sind, und diese Übermittlungen ohne weitere Genehmigung des Verantwortlichen durchzuführen. Kommt dieser andere Datenverarbeiter seinen Verpflichtungen in Bezug auf den Schutz personenbezogener Daten nicht nach, so bleibt der Auftragsverarbeiter gegenüber dem Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen dieses anderen Datenverarbeiters verantwortlich.

7. Unterstützung

a. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten gemäß Artikel 32 bis 36 der DSGVO (oder den gleichwertigen Abschnitten des geltenden Rechts) unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

b. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen im Rahmen des Möglichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Verpflichtung des Verantwortlichen zur Beantwortung von Anfragen zur Ausübung der Rechte der betroffenen Person gemäß der DSGVO. Der Auftragsverarbeiter leitet jede Anfrage einer betroffenen Person in Bezug auf personenbezogene Daten unverzüglich an den Verantwortlichen weiter.

c. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei allen Datenschutz-Folgenabschätzungen und Konsultationen und Mitteilungen mit den Aufsichtsbehörden gemäß der DSGVO.

8. Verletzung des Schutzes personenbezogener Daten

a. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, nachdem er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt.

b. Die Benachrichtigung des Auftragsverarbeiters über eine Verletzung des Schutzes personenbezogener Daten muss mindestens:

   i. die Art der Verletzung des Schutzes personenbezogener Daten beschreiben, einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl der betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen Datensätze personenbezogener Daten;

   ii. den Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters oder einer anderen Kontaktstelle angeben, bei dem bzw. der weitere Informationen eingeholt werden können;

   iii. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten beschreiben; und

   iv. die Maßnahmen beschreiben, die der Auftragsverarbeiter ergriffen hat oder zu ergreifen gedenkt, um die Verletzung des Schutzes personenbezogener Daten zu beheben, gegebenenfalls einschließlich der Maßnahmen zur Abmilderung möglicher negativer Auswirkungen.

c. Wenn und soweit es nicht möglich ist, die verlangten Informationen gleichzeitig zu übermitteln, können die Informationen ohne unangemessene Verzögerung nach und nach übermittelt werden.

d. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Dokumentation und Reaktion auf eine Verletzung des Schutzes personenbezogener Daten, insbesondere bei der Kommunikation mit den betroffenen Personen gemäß Artikel 34 der DSGVO (oder einer nach geltendem Recht gleichwertigen Bestimmung).

9. Löschung oder Rückgabe personenbezogener Daten

a. Nach Wahl des Verantwortlichen löscht der Auftragsverarbeiter nach Beendigung der Erbringung von Dienstleistungen im Zusammenhang mit der Verarbeitung alle personenbezogenen Daten oder gibt sie an den Verantwortlichen zurück, löscht vorhandene Kopien und löscht oder entsorgt sicher alle Datenträger sowie alle Probe- und Abfallmaterialien, die solche Kopien enthalten.

b. Ungeachtet des Vorstehenden kann der Auftragsverarbeiter, solange er die personenbezogenen Daten weiterhin gemäß den Standards des anwendbaren Rechts und dieser DPA schützt:

   i. angemessene Kopien der personenbezogenen Daten aufbewahren, die zur Erfüllung geltender gesetzlicher, behördlicher, gerichtlicher, prüfungsbezogener oder interner Compliance-Anforderungen erforderlich sind;

   ii. personenbezogene Daten in dem Umfang und so lange aufbewahren, wie dies nach geltendem Recht erforderlich ist; und

   iii. personenbezogene Daten in dem Umfang und so lange aufbewahren, wie sie nicht auf vernünftige und praktikable Weise aus den Systemen gelöscht werden können (z. B. in automatischen Backups, latenten Daten, Metadaten und Daten, die ganz, teilweise oder gemeinsam im Besitz anderer Unternehmen sind).

c. Falls der Auftragsverarbeiter personenbezogene Daten nach Ablauf oder Beendigung dieser DPA aufbewahrt, löscht oder gibt er alle diese personenbezogenen Daten unverzüglich zurück, sobald die Bedingungen, unter denen die Aufbewahrung erforderlich war, dies zulassen. Die Bestimmungen dieser DPA gelten für alle personenbezogenen Daten, die auf diese Weise gespeichert werden, solange sie gespeichert werden.

d. Alle zusätzlichen Kosten, die im Zusammenhang mit der Rückgabe oder Löschung personenbezogener Daten nach Beendigung oder Ablauf dieser DPA entstehen, werden vom Verantwortlichen getragen.

10. Audits und Inspektionen

a. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Verpflichtungen gemäß der DSGVO und dieser DPA nachzuweisen, und ermöglicht und unterstützt Audits, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen vom Verantwortlichen beauftragten Prüfer durchgeführt werden.

b. Die Parteien vereinbaren, dass für jedes Jahr, in dem der Auftragsverarbeiter keine Verletzung des Schutzes personenbezogener Daten verursacht hat, der Auftragsverarbeiter die oben genannten Informationspflichten erfüllen kann, indem er dem Verantwortlichen eine Kopie des aktuellen Berichts eines unabhängigen Prüfers über die Betriebskontrollen des Auftragsverarbeiters vorlegt.

c. Audits oder Inspektionen durch oder im Namen des Verantwortlichen beschränken sich auf Informationen, die unmittelbar für die Einhaltung dieser DPA relevant sind, und werden nach angemessener schriftlicher Vorankündigung während der üblichen Geschäftszeiten und unter Einhaltung der Betriebs-, Sicherheits- und Vertraulichkeitsanforderungen des Auftragsverarbeiters durchgeführt.

d. Jeder vom Verantwortlichen ausgewählte externe Prüfer muss mit dem Auftragsverarbeiter eine Vertraulichkeitsvereinbarung abschließen, bevor er Zugang zu Informationen oder Einrichtungen des Auftragsverarbeiters erhält.

11. Laufzeit

Die Laufzeit dieser DPA und der Verarbeitung beginnt mit dem Datum des Inkrafttretens und dauert bis zum Ablauf oder der Kündigung des Vertrags.

12. Kündigung

Jede Partei kann diese DPA kündigen und die Kündigungsbestimmungen des Vertrags aus wichtigem Grund geltend machen, wenn die andere Partei eine Bestimmung dieser DPA wesentlich verletzt oder gegen anwendbare Bestimmungen der DSGVO oder des Datenschutzrechts der Europäischen Union oder eines Landes verstößt.

13. Fortbestand von Bestimmungen

Die Abschnitte dieser DPA mit den Überschriften „Vertraulichkeit“, „Unterstützung“, „Löschung oder Rückgabe personenbezogener Daten“, „Geltendes Recht“, „Salvatorische Klausel“ und „Kein Verzicht“ sowie alle anderen Bestimmungen, die den Ablauf oder die Kündigung dieser DPA überdauern sollen, um ihrem Zweck gerecht zu werden, bleiben auch nach Ablauf oder Kündigung dieser DPA in Kraft.

14. Mitteilungen

Alle rechtsverbindlichen Mitteilungen im Rahmen dieser DPA bedürfen der Schriftform und müssen wie im Vertrag vorgesehen zugestellt werden. Eine Kopie jeder rechtsverbindlichen Mitteilung ist dem General Counsel der empfangenden Partei zuzustellen.

15. Geltendes Recht

a. Die DSGVO regelt alle Angelegenheiten, die sich aus dieser DPA ergeben oder mit ihr in Zusammenhang stehen.

b. Ungeachtet des Vorstehenden gelten in den Fällen, in denen die DSGVO die Anwendung anderer Gesetze als der DSGVO, anderer Gesetze der Europäischen Union oder Gesetze der Mitgliedstaaten zulässt, das anwendbare Recht, die Gerichtsbarkeit und der Gerichtsstand wie im Vertrag festgelegt.

16. Gesamter Vertrag

Diese DPA und der Vertrag stellen die gesamte Übereinkunft zwischen den Parteien in Bezug auf den hierin behandelten Gegenstand dar und ersetzen alle früheren Verhandlungen, Vereinbarungen und Absprachen zwischen den Parteien, ob schriftlich oder mündlich, in Bezug auf den hierin behandelten Gegenstand. Im Falle eines Widerspruchs zwischen den Bestimmungen oder Bedingungen dieser DPA und dem Vertrag haben die Bestimmungen dieser DPA Vorrang vor den widersprüchlichen Bestimmungen oder Bedingungen des Vertrags. Diese DPA kann nur durch ein von beiden Parteien unterzeichnetes Schriftstück geändert werden.

17. Salvatorische Klausel

Sollte eine Bestimmung dieser DPA in einer Rechtsordnung ungültig, rechtswidrig oder nicht durchsetzbar sein, so hat dies keine Auswirkungen auf die übrigen Bestimmungen dieser DPA und führt nicht dazu, dass diese Bestimmungen in anderen Rechtsordnungen ungültig oder nicht durchsetzbar sind. Sollte ein zuständiges Gericht feststellen, dass eine Bestimmung dieser DPA ungültig, rechtswidrig oder nicht durchsetzbar ist, kann das Gericht diese DPA so ändern, dass sie dem geltenden Recht und der ursprünglichen Absicht der Parteien so weit wie möglich entspricht.

18. Überschriften

Die Überschriften in dieser DPA dienen lediglich der Übersichtlichkeit und sind nicht als Teil dieser DPA gedacht oder sollen die Auslegung dieser DPA beeinflussen.

19. Kein Verzicht

Der Verzicht einer Partei auf die Geltendmachung eines Verstoßes gegen eine Bestimmung dieser DPA kann nicht als Verzicht dieser Partei auf die Geltendmachung eines späteren Verstoßes ausgelegt werden.

Beschreibung der Kontrollen des Auftragsverarbeiters

Der Auftragsverarbeiter ist verpflichtet, seine technischen und organisatorischen Maßnahmen aufrechtzuerhalten und zu aktualisieren, um die nachstehend beschriebenen Anforderungen und die anwendbaren Gesetze zu erfüllen oder zu übertreffen.

1. **Unbefugter Zugriff**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um zu verhindern, dass Unbefugte Zugriff auf Datenverarbeitungssysteme erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

Der Auftragsverarbeiter wendet Kontrollen für die Benutzerzugriffsverwaltung, die System- und Anwendungszugriffsverwaltung, physische und umgebungsbezogene Sicherheitskontrollen sowie organisatorische Rollen, Verantwortlichkeiten und Befugnisse an. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Überwachungen, Analysen und Bewertungen durch. Der Auftragsverarbeiter schult das Personal bei der Einstellung und einmal jährlich und unterhält Richtlinien- und Verfahrensdokumente, die Hinweise zum unberechtigten Zugriff geben.

2. **Unbefugte Nutzung**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um eine unbefugte Nutzung der Datenverarbeitungssysteme zu verhindern:

Der Auftragsverarbeiter wendet Kontrollen für die Benutzerzugriffsverwaltung, die System- und Anwendungszugriffsverwaltung, kryptografische Kontrollen, physische und umgebungsbezogene Sicherheitskontrollen, organisatorische Rollen, Verantwortlichkeiten und Befugnisse an. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Überwachungen, Analysen und Bewertungen durch. Der Auftragsverarbeiter schult das Personal bei der Einstellung und einmal jährlich und unterhält Richtlinien- und Verfahrensdokumente, die Hinweise zur unberechtigten Nutzung geben.

3. **Eingeschränkte Rechte**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um zu gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung oder Nutzung oder nach ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

Der Auftragsverarbeiter hat Kontrollen für die Registrierung und Abmeldung von Benutzern, die rollenbasierte Bereitstellung von Benutzerzugriffsrechten, die Verwaltung privilegierter Zugriffsrechte, die Überprüfung von Benutzerzugriffsrechten und die Aufhebung oder Anpassung von Zugriffsrechten bei Rollenwechsel implementiert. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Überwachungen, Analysen und Bewertungen durch. Die Schulung des Personals des Auftragsverarbeiters umfasst Hinweise zu eingeschränkten Rechten.

4. **Übermittlung**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übermittlung oder beim Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden sollen:

Um eine sichere Datenübermittlung zu gewährleisten, verwendet der Auftragsverarbeiter Secure Hypertext Transfer Protocol (HTTPS), File Transfer Protocol Secure (FTPS) und Virtual Private Network (VPN), um die standardmäßige Übermittlung personenbezogener Daten im Rahmen seiner Produkte und Dienste zu schützen. Für diese Methoden sind Benutzer-IDs und Passwörter und in einigen Fällen eine Multi-Faktor-Authentifizierung erforderlich. Der Auftragsverarbeiter verwendet bei Bedarf eine Verschlüsselung, die den Standards des US-amerikanischen National Institute of Standards and Technology (NIST) entspricht. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Überwachungen, Analysen und Bewertungen durch.

5. **Prüfpfade**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um zu gewährleisten, dass überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt wurden:

Der Auftragsverarbeiter unterhält Prüfpfade, um kritische Ereignisse für seine wichtigsten IT-Infrastrukturkomponenten und Anwendungen zu protokollieren. Der Auftragsverarbeiter unterhält auch eine Reihe von Sicherheitssoftware, einschließlich:
(1) Fernzugriffssoftware, (2) Web-Proxys und (3) Authentifizierungsserver, die eine Quelle für Computersicherheitsprotokolldaten sind. Der Auftragsverarbeiter verwendet Protokolle, um Benutzeraktionen aufzuzeichnen und Daten bereitzustellen, die für die Untersuchung böswilliger Aktivitäten nützlich sind.

6. **Unterauftragnehmer**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass im Fall der Verarbeitung personenbezogener Daten durch einen Unterauftragsverarbeiter die Daten streng nach den Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet werden:

Der Auftragsverarbeiter unterhält schriftliche Verträge mit seinen Unterauftragnehmern, in denen die zu erbringenden Dienstleistungen festgelegt sind, und führt Kontrollen in Bezug auf die Verarbeitung personenbezogener Daten durch, einschließlich der Verpflichtung zur Einhaltung von Anweisungen. Der Auftragsverarbeiter schließt bei Bedarf Datenverarbeitungsverträge und Standardvertragsklauseln mit Unterauftragsverarbeitern ab. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Kontrollen, Analysen und Bewertungen von Unterauftragnehmern durch. Der Auftragsverarbeiter stellt in seinen Richtlinien und Verfahren Leitlinien für das Management von Unterauftragnehmern zur Verfügung.

7. **Verfügbarkeit**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass personenbezogene Daten vor zufälliger Zerstörung oder zufälligem Verlust geschützt sind:

Der Auftragsverarbeiter verwendet Datenverarbeitungseinrichtungen, die für eine hohe Verfügbarkeit redundant ausgelegt sind. Der Verarbeiter überwacht und optimiert seine Verarbeitungsprozesse und erstellt Prognosen über den zukünftigen Kapazitätsbedarf, um die Systemleistung aufrechtzuerhalten. Der Auftragsverarbeiter unterhält Verfahren für die Datensicherung und -wiederherstellung, das Änderungsmanagement, die Geschäftskontinuität und Notfallwiederherstellung, die Datenlöschung und Medienwiederherstellung sowie die Reaktion auf Sicherheits- und Datenschutzvorfälle. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Überwachungen, Analysen und Verfügbarkeitsbewertungen durch.

8. **Getrennte Verarbeitung**: Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um sicherzustellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt voneinander verarbeitet werden können:

Der Auftragsverarbeiter hält die getrennte Verarbeitung aufrecht, indem er die technischen Möglichkeiten der eingesetzten Software (z. B. Mandantenfähigkeit oder getrennte Systemlandschaften) nutzt, um eine Trennung der Daten zwischen den Kunden zu erreichen. Es sind geeignete Verfahren und Maßnahmen vorhanden, um die Verarbeitung der erhobenen Daten auf die im Rahmen der Kundenvereinbarung zulässigen Zwecke zu beschränken und eine getrennte Datenverarbeitung sicherzustellen. Der Auftragsverarbeiter führt regelmäßig Risikobewertungen sowie Kontrollen, Analysen und Bewertungen der getrennten Verarbeitung durch.