Anlage Auftragsverarbeitung (Verantwortlicher-Auftragsverarbeiter)

Diese Anlage Auftragsverarbeitung, welche die Bedingungen für die Auftragsverarbeitung und die Beschreibung der Technischen und Organisatorischen Maßnahmen (TOM) des Auftragsverarbeiters mit umfasst (Auftragsverarbeitungsvereinbarung – "AVV"), ist Bestandteil des Vertrages zwischen dem Nutzer und GHX, insoweit handelnd als Verantwortlicher und Auftragsverarbeiter. Die Parteien vereinbaren diesbezüglich was folgt:

1. Begriffsbestimmungen und Angaben zu den Datenverarbeitungen

Zusätzlich zu den Begriffsbestimmungen im Vertrag gelten die nachfolgenden Begriffsbestimmungen. Ergänzend zu den Begriffsbestimmungen im Vertrag und den nachfolgenden Begriffsbestimmungen gelten die Begriffsbestimmungen der DSGVO (wie nachfolgend definiert).

Begriff	Bedeutung
Datenkategorien	Kontaktdaten; Personaldaten; gesundheitsbezogene Daten; IT-System-Informationen; Inhalte und Telekommunikationsdaten von E-mails; Einzelheiten von Waren und Dienstleistungen; Finanzdaten.
Betroffene	• Frühere, gegenwärtige und künftige Arbeitnehmer, Auftragnehmer, Zulieferer und Vertriebsmittler des Verantwortlichen; • Frühere, gegenwärtige und künftige Patienten des Verantwortlichen und deren Angehörige, Betreuer und Pfleger.
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
Personenbezogene Daten	die personenbezogen Daten wie in der DSGVO definiert, die vom Auftragsverarbeiter für den Verantwortlichen verarbeitet werden.
Verarbeitungen	jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Personenbezogenen Daten
Ort der Verarbeitungen	• Die Betriebsstätten des Auftragsverarbeiters in Cambridge, Vereinigtes Königreich; Brüssel, Belgien; Düsseldorf, Frankfurt, Königstein im Taunus, und Koblenz, Deutschland; Hilversum, Niederlande; Baar, Schweiz und Louisville, Colorado, USA. • Die Betriebsstätten der Auftragnehmer des Auftragsverarbeiters in der EU/ im EWR; im Vereinigten Königreich; Kanada; Texas; Virginia und Washington in den USA; Indien.
Zwecke der Verarbeitung	• für berechtigte Interessen des Verantwortlichen, seiner Zuliefer, Vertragspartner oder Vertriebsmittler, oder des Auftragsverarbeiters in Umsetzung des Vertrages • die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im

	Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in der DSGVO genannten Bedingungen und Garantien bzgl. der Verarbeitung durch Fachpersonal oder unter dessen Verantwortung, wobei dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder durch eine andere Person, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.
AVV	Diese Anlage Auftragsverarbeitung, bestehend aus diesem Deckblatt und den folgenden Anlagen, die Bestandteil des Vertrages sind: 1. die Bedingungen für die Auftragsverarbeitung; 2. die Beschreibung der Technischen und Organisatorischen Maßnahmen (TOM) des Auftragsverarbeiters
Verantwortlicher	Der Nutzer, zusammen mit seinen Konzernunternehmen wie im Vertrag bezeichnet.
Auftragsverarbeiter	Die GHX-Gesellschaft, die Partei des Vertrages ist.
Vertrag	Der Vertrag bzw. die Verträge über die Erbringung von Dienstleistungen zwischen den Parteien bzw. deren verbundenen Unternehmen einschließlich aller Nachträge, Zusätze, Anlagen, Anhänge und Einzelaufträge.

Bedingungen für die Auftragsverarbeitung

2. Einbeziehung in den Vertrag

Die Parteien vereinbaren hiermit, diese AVV mit Wirkung zum Inkrafttreten des Vertrages („Datum des Inkrafttretens“) zu dessen Bestandteil zu machen.

3. Auftragsverarbeitungen

a. Der Auftragsverarbeiter verareitet die Personenbezogenen Daten ausschließlich gemäß dokumentierten Weisungen des Verantwortlichen und in Übereinstimmung mit dem Vertrag, auch in Bezug auf die Übermittlung Personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

b. Der Vertrag und diese AVV stellen die allgemeinen Weisungen des Verantwortlichen im Hinblick auf die Verarbeitung Personenbezogener Daten dar. Der Verantwortliche kann jederzeit ergänzend konkrete Weisungen erteilen, die die Verarbeitungen einschränken, soweit diese mit dem anwendbaren Recht übereinstimmen.

c. Der Auftragsverarbeiter darf Personenbezogene Daten nicht für andere Zwecke als die auf dem Deckblatt angegebenen Zwecke verarbeiten, soweit der Verantwortliche diese nicht vorher geprüft und schriftlich freigegeben hat.

d. Jede Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung von Personenbezogenen Daten erfolgt ausschließlich gemäß den Weisungen des Verantwortlichen.

e. Sollte der Auftragsverarbeiter im Hinblick auf die Festlegung der Zwecke und der Mittel zur Verarbeitung Personenbezogener Daten zusammen dem Verantwortlichen als gemeinsam für die Verarbeitung Verantwortlicher nach DSGVO anzusehen sein, wird der Auftragsverarbeiter zusätzlich alle gesetzlichen Pflichten des Verantwortlichen im Hinblick auf solche Personenbezogene Daten erfüllen. In diesen Fällen bleibt der Verantwortliche der Ansprechpartner für die Betroffenen.

f. Beide Parteien sind verpflichtet, bei Ausführung dieser AVV und des Vertrages das anwendbare Recht, insbesondere die DSGVO zu beachten.

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

4. Vertraulichkeit

a. Der Auftragsverarbeiter hat die Vertraulichkeit Personenbezogener Daten in Übereinstimmung mit dem anwendbaren Recht und dem Vertrag unter Einsatz wirtschaftlich angemessener Sicherungsvorkehrungen zu wahren.

b. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

c. Dem Auftragsverarbeiter ist bekannt und er stimmt zu, dass der Verantwortliche oder seine Kommunikationspartner im Hinblick auf genetische Daten, biometrische Daten und Gesundheitsdaten, die mittels der Dienste des Auftragsverarbeiters übermittelt werden, einer gesetzlichen Verschwiegenheitsverpflichtung (Berufsgeheimnis) nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen unterliegen und dass diese Geheimhaltungspflicht bei der betreffenden Datenverarbeitung auch für ihn gilt.

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 trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

   i. die Pseudonymisierung und Verschlüsselung Personenbezogener Daten;

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

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

   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 Schutzniveaus hat der Auftragsverarbeiter insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu Personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

c. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 der DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 der DSGVO kann als Faktor herangezogen werden, um die Erfüllung der in dieser AVV vereinbarten Anforderungen an die technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter nachzuweisen. Der Auftragsverarbeiter hat dem Verantwortlichen insoweit eine aktuelle Dokumentation der Erfüllung der vereinbarten Anforderungen zur Verfügung zu stellen und diese unverzüglich bei jeder wesentlichen Änderung zu aktualisieren.

d. Der Auftragsverarbeiter hat Schritte zu unternehmen, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu Personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

e. Der Auftragsverarbeiter hat Richtlinien aufgestellt und umgesetzt, um die Anforderungen der DSGVO, des Mitgliedstaates und anderer Datenschutzgesetze, der Anlage „Beschreibung der Technischen und Organisatorische Maßnahmen (TOM) des Auftragsverarbeiters“ und anderer anwendbarer gesetzlicher Bestimmungen umzusetzen. Der Auftragsverarbeiter stellt dem Verantwortlichen auf schriftliches Verlangen jederzeit Kopien dieser Richtlinien zur Verfügung.

6. Weitere Auftragsverarbeiter

a. Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Es besteht Einigkeit zwischen den Parteien, dass die Bestimmungen des Vertrages im Hinblick auf die ausdrückliche Zulassung von Unterbeauftragungen auch als allgemeine Genehmigung des Verantwortlichen im Hinblick auf die Inanspruchnahme von Konzernunternehmen und von Dienstleistern im Bereich Outsourcing von Geschäftsprozessen. IT-Leistungen, Hosting oder Speicherung von Daten, Telekommunikation, Rechtsberatung und Buchhaltung als weitere Auftragsverarbeiter darstellt. Auf schriftliches Verlangen des Verantwortlichen wird der Auftragsverarbeiter den Verantwortlichen - höchstens ein Mal pro Jahr - davon informieren wenn weitere Auftragsverarbeiter, die nicht nur gelegentlich auf Personenbezogene Daten zugreifen, ergänzt oder ersetzt werden.

b. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so hat er diesem weiteren Auftragsverarbeiter im Wege eines schriftlichen Vertrags mindestens gleichwertige Datenschutzpflichten aufzuerlegen, wie sie in dieser AVV, dem Vertrag oder einer sonstigen Vereinbarung zwischen den Parteien nach der AVV oder DSGVO festgelegt sind. In

diesem Vertrag sind hinreichende Garantien dafür vorzusehen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser AVV, der DSGVO und sonstiger anwendbarer gesetzlicher Bestimmungen erfolgt. Soweit der weitere Auftragsverarbeiter sich in einem Drittland befindet, welches kein angemessenes Datenschutzniveau bietet, muss der Vertrag ein angemessenes Schutzniveau sicherstellen (z.B. durch Verwendung der Standardvertragsklauseln). Der Verantwortliche autorisiert den Auftragsverarbeiter hiermit, Standardvertragsklauseln mit weiteren Auftragsverarbeitern der vorgenannten Kategorien im Hinblick auf Übermittlungen Personenbezogener Daten in die unter „Ort der Verarbeitungen“ auf dem Deckblatt genannten Länder abzuschließen und solche Übermittlungen ohne weitere gesonderte Zustimmung des Verantwortlichen vorzunehmen. Kommt der weitere Auftragsverarbeiter seinen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

7. Unterstützung

a. The Auftragsverarbeiter hat den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen zu unterstützen.

b. Der Auftragsverarbeiter hat angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in der DSGVO genannten Rechte der Betroffenen Person nachzukommen. Der Auftragsverarbeiter leitet Anfragen der Betroffenen in Bezug auf Personenbezogene Daten unverzüglich an den Verantwortlichen weiter.

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

8. Verletzung des Schutzes Personenbezogener Daten

a. Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes Personenbezogener Daten unverzüglich nachdem ihm diese bekannt wurde.

b. Die Meldung des Auftragsverarbeiters enthält zumindest folgende Informationen:

   i. eine Beschreibung der Art der Verletzung des Schutzes Personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   ii. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle des Auftragsverarbeiters für weitere Informationen;

   iii. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten

   iv. eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

c. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Auftragsverarbeiter diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

d. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Dokumentation und Bearbeitung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 34 der DSGVO einschließlich der Kommunikation mit den Betroffenen.

9. Löschung oder Rückgabe Personenbezogener Daten

a. Nach Wahl des Verantwortlichen hat der Auftragsverarbeiter bei Beendigung des Auftrages alle Personenbezogene Daten an den Verantwortlichen zurückzugeben oder zu löschen, alle Kopien zu löschen und Datenträger datenschutzgerecht zu löschen oder zu vernichten. Gleiches gilt für entsprechendes Test- und Ausschussmaterial.

b. Unbeschadet dessen ist der Auftragsverarbeiter unter der Voraussetzungen, dass er deren Schutz in Übereinstimmung mit dieser AVV und dem anwendbaren Recht aufrechterhält, berechtigt:

i. Kopien Personenbezogener Daten zur Einhaltung gesetzlicher, regulatorischer oder gerichtlicher Anforderungen oder interner Prüfungs- und Compliance-Vorgaben aufzubewahren,

ii. Personenbezogene Daten aufzubewahren, soweit und solange dies gesetzlich geboten ist und

iii. Personenbezogene Daten aufzubewahren, soweit und solange eine Löschung von den Systemen unmöglich oder unzumutbar ist (bspw. im Hinblick auf Sicherungskopien, Latent Data, Metadaten und Daten die ganz oder teilweise auch anderen Unternehmen zustehen).

c. Soweit der Auftragsverarbeiter Personenbezogene Daten nach Beendigung dieser AVV durch Zeitablauf oder Kündigung zurückbehält, sind diese unverzüglich zu löschen oder zurückzugeben, sobald die Voraussetzungen für die Zurückbehaltung nicht mehr vorliegen. Die Bestimmungen dieser AVV gelten weiter für Personenbezogene Daten, solange diese beim Auftragsverarbeiter verbleiben.

d. Zusätzliche Kosten im Zusammenhang mit der Rückgabe oder Löschung Personenbezogener Daten nach Beendigung dieser AVV durch Zeitablauf oder Kündigung trägt der Verantwortliche.

10. Auditierungen und Prüfungen

a. Der Auftragsverarbeiter stellt dem Verantwortlichen alle informationen zu Verfügung, die erforderlich sind, um die Einhaltung der Anforderungen der DSGVO und dieser AVV zu verifizieren. Er ermöglicht Auditierungen und Prüfungen durch den Verantwortlichen oder von diesem beauftragte Prüfer und unterstützt diese.

b. Es besteht Einigkeit zwischen den Parteien, dass der Auftragsverabeiter berechtigt ist, für jedes Jahr, in welchem er keine Verletzung des Schutzes Personenbezogener Daten verursacht, den vorstehend vereinbarten Nachweis durch Vorlage eines aktuellen Berichts eines externen Prüfers über die getroffenen technischen und organisatorischen Maßnahmen zu führen.

c. Alle Auditierungen und Prüfungen des Verantwortlichen sind auf Informationen, die für die Einhaltung dieser AVV unmittelbar relevant sind, zu beschränken, angemessen vorher anzukündigen und zu normalen Geschäftszeiten und unter Beachtung der Anforderungen des Auftragsverarbeiters im Hinblick auf Geschäftsabläufe, Sicherheit und Vertraulichkeit durchzuführen.

d. Der vom Verantwortlichen beauftragte Prüfer hat vor Zugang zu Informationen oder Betriebsstätten eine Vertraulichkeitsvereinbarung mit dem Auftragsverarbeiter abzuschließen.

11. Laufzeit

Die Laufzeit dieser AVV beginnt mit dem Datum des Inkrafttretens und läuft bis zur Beendigung des Vertrages durch Zeitablauf oder Kündigung.

12. Kündigung

Beide Parteien sind berechtigt, diese AVV aus wichtigem Grund zu kündigen und auch von dem Kündigungsverfahren aus wichtigem Grund gemäß dem Vertrag Gebrauch zu machen, wenn die jeweils andere Partei Bestimmungen dieser AVV, der DSGVO oder sonstigen anwendbaren Rechts der Union oder nationalen Rechts zum Datenschutz wesentlich verletzt.

13. Fortgeltung

Die Abschnitte dieser AVV „Vertraulichkeit“, „Unterstützung“, „Löschung oder Rückgabe Personenbezogener Daten“, “Anwendbares Recht”, “Teilnichtigkeit” und “Kein Verzicht” sowie andere Bestimmungen, die nach ihrem Wortlaut oder Sinn auch nach Kündigung weiter gelten sollen, gelten auch nach Beendigung dieser AVV durch Zeitablauf oder Kündigung fort.

14. Erklärungen

Erklärungen im Zusammenhang mit dieser AVV bedürfen der Schriftform und sind in der im Vertrag vereinbarten Form mitzuteilen. Erklärungen zur Ausübung von Gestaltungsrechten sind in Kopie an den Leiter der Rechtsabteilung der Gegenpartei zu übersenden.

15. Anwendbares Recht

a. Diese AVV unterliegt der DSGVO.

b. Soweit die DSGVO Regelungen zulassen, die von der DSGVO bzw. dem Recht der Union oder der Mitgliedstaaten abweichen, finden die Bestimmungen des Vertrages in Bezug auf das

anwendbare Recht, die Streitentscheidung und gerichtliche Zuständigkeit auch auf diese AVV Anwendung.

16. Vollständigkeit

Diese AVV und der Vertrag enthalten sämtliche Vereinbarungen der Parteien in Bezug auf den Vertragsgegenstand und ersetzen alle früheren Verhandlungen, Vereinbarungen und Abreden zwischen den Parteien, gleich ob mündlich oder schriftlich, in Bezug auf den Vertragsgegenstand. Im Falle eines Widerspruchs zwischen den Bestimmungen dieser AVV und des Vertrages gehen die Bestimmungen dieser AVV den widersprechenden Bestimmungen des Vertrages vor. Änderungen dieser AVV bedürfen der Schriftform.

17. Teilnichtigkeit

Soweit eine Bestimmung dieser AVV in irgendeiner Rechtsordnung unwirksam, rechtswidrig oder undurchsetzbar sein sollte, berührt dies weder die Wirksamkeit und Durchsetzbarkeit der übrigen Bestimmungen dieser AVV noch die Wirksamkeit und Durchsetzbarkeit der betroffenen Bestimmung(en) in einer anderen Rechtsordnung. Soweit ein zuständiges Gericht eine Bestimmung dieser AVV als unwirksam, rechtswidrig oder undurchsetzbar verwirft, ist es berechtigt, diese durch eine Regelung zu ersetzen, die dem von den Parteien ursprünglich beabsichtigten Ergebnis so nahe wie möglich kommt.

18. Überschriften

Die Überschriften dieser AVV dienen nur der Übersicht und sind für die Auslegung dieser AVV nicht maßgeblich.

19. Kein Verzicht

Der Verzicht einer Partei im Hinblick auf die Nichteinhaltung einer Bestimmung dieser AVV gilt nur für den Einzelfall und begründet keinen Verzicht im Hinblick auf die künftige Einhaltung.

Beschreibung der Technischen und Organisatorische Maßnahmen (TOM) des Auftragsverarbeiters

Der Auftragsverarbeiter hat technische und organisatorische Maßnahmen zu unterhalten und zu aktualisieren, die mindestens die Einhaltung der nachfolgenden Anforderungen sowie aller anwendbaren gesetzlichen Anforderungen sicherstellen.

1. **Zutrittskontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Der Auftragsverarbeiter unterhält technische und organisatorische Verfahren für die Verwaltung von Benutzer-, System- und Anwendungszugängen, physische Zugangs- und Umweltsicherheitskontrollen und Rollenkonzepte zur Zuweisung von Rollen, Verantwortlichkeiten und Kompetenzen. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen durch. Der Auftragsverarbeiter schult alle Mitarbeiter bei der Einstellung und danach mindestens jährlich und unterhält interne Richtlinien und Verfahren zur Vermeidung des unbefugten Zutritts.

2. **Zugangskontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Der Auftragsverarbeiter unterhält technische und organisatorische Verfahren für die Verwaltung von Benutzer-, System- und Anwendungszugängen, kryptographische Kontrollen, physische Zugangs- und Umweltsicherheitskontrollen und Rollenkonzepte zur Zuweisung von Rollen, Verantwortlichkeiten und Kompetenzen. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen durch. Der Auftragsverarbeiter schult alle Mitarbeiter bei der Einstellung und danach mindestens jährlich und unterhält interne Richtlinien und Verfahren zur Vermeidung des unbefugten Zugangs.

3. **Zugriffskontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Der Auftragsverarbeiter unterhält technische und organisatorische Verfahren für die Registrierung und De-Registrierung von Nutzern, Rollenbasierte Zugriffsrechte, die Verwaltung abgestufter Zugriffsrechte, die Überprüfung von Zugriffsrechten und Entzug oder Einschränkung von Zugriffsrechten bei Rollenwechseln. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen durch. Der Auftragsverarbeiter schult alle Mitarbeiter bei der Einstellung und danach mindestens jährlich und unterhält interne Richtlinien und Verfahren zur Beschränkung von Zugriffen.

4. **Weitergabekontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Zur Wahrung der Übertragungssicherheit verwendet der Auftragsverarbeiter den Schutz durch Secure Hypertext Transfer Protocol (HTTPS), File Transfer Protocol Secure (FTPS), oder Virtual Private Network (VPN) für regelmäßige Übertragungen Personenbezogener Daten im Rahmen seiner Produkte und Dienstleistungen. Diese Verfahren erfordern die Eingabe von Kennungen und Passwörtern und z.T. auch Multi-Factor Authentication *(MFA). Der Auftragsverarbeiter nutzt, soweit angemessen, Verschlüsselungsverfahren, die die Standards der US National Institute of Standards and Technology (NIST) erfüllen. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen durch.*

5. **Eingabekontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Für kritische Verarbeitungen werden im Rahmen der wesentlichen IT-Infrastruktur, IT-Komponenten und Anwendungen Protokolldateien verwendet. Der Auftragsverarbeiter verwendet verschiedene Sicherheitstechnologien, u.a. (1) Remote Access Software; (2) Web-Proxies und (3) Authentication Servers als Quelle von Computersicherheitslogs. Der Auftragsverarbeiter erzeugt und nutzt Protokolldateien zur Protokollierung von Nutzeraktivitäten und Prüfung von Missbräuchen.

6. **Auftragskontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die von weiteren Auftragsverarbeitern im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können:

Der Auftragsverarbeiter schließt mit Dienstleistern und weiteren Auftragsverarbeitern schriftliche Verträge ab, die die Dienste und die technischen und organisatorischen Maßnahmen im Hinblick auf die Verarbeitung Personenbezogener Daten festlegen, insbesondere das Erfordernis der Einhaltung von Weisungen. Soweit erforderlich werden Auftragsverarbeitungsvereinbarungen und Standardvertragsklauseln abgeschlossen. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen durch. Der Auftragsverarbeiter unterhält interne Richtlinien und Verfahren zur Überwachung von Unterauftragnehmern.

7. **Verfügbarkeitskontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Der Auftragsverarbeiter nutzt Datenverarbeitungsanlagen, bei denen eine hohe Verfügbarkeit durch Redundanz gesichert ist. Der Auftragsverarbeiter überwacht und steuert die Datenverarbeitungen laufend und plant künftige Systemkapazitätserfordernisse, um die Systemleistung zu erhalten. Der Auftragsverarbeiter unterhält Verfahren für die Datensicherung und –wiederherstellung, das Change Management, die Überbrückung von Ausfällen und Notfällen, die Datenlöschung und Datenträgerentsorgung sowie für die Reaktion auf Verletzungen des Schutzes Personenbezogener Daten. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen im Hinblick auf die Verfügbarkeit durch.

8. **Trennungskontrolle:** Der Auftragsverarbeiter unterhält die folgenden technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Trennung von Datenbeständen unterschiedlicher Auftraggeber erfolgt durch den Auftragsverarbeiter unter Nutzung der technischen Verfahren der eingesetzten Software (z.B. Mandantenfähigkeit, getrennte Systemlandschaften). Der Auftragsverarbeiter ergreift technische und organisatorische Maßnahmen, um die Verarbeitungen auf die Zwecke der verschiedenen Verträge zu beschränken und zu trennen. Der Auftragsverarbeiter führt regelmäßig Risikoabschätzungen und Kontrollen, Analysen und Evaluierungen im Hinblick auf die Trennung von Datenbeständen durch.