Art der Information: Eingeschränkt

Version: 2023-10

Auftragsverarbeitungsvertrag (AVV)

gemäß Artikel 28 (3) DSGVO
für Wartungsdienste

zwischen:
Auftraggeber (gemäß Softwarepflege-Vertrag)

und:

NTT DATA Business Solutions AG
Königsbreede 1
33605 Bielefeld

(im Folgenden als "**Auftragnehmer**" bezeichnet)

§ 1 Präambel und Anwendungsbereich

Der Auftragnehmer verarbeitet personenbezogene Daten im Rahmen seiner Dienstleistungen für den Auftraggeber gemäß Artikel 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutzgrundverordnung - "DSGVO").

Die in diesem Vertrag verwendeten Begriffe werden in Übereinstimmung mit ihrer Definition in der DSGVO verwendet. Sofern in diesem Vertrag oder in den geltenden gesetzlichen Bestimmungen nicht ausdrücklich etwas anderes vorgesehen ist, genügt für die Abgabe einer schriftlichen Erklärung auch die elektronische Form (z. B. E-Mail).

§ 2 Vertragsgegenstand und Laufzeit des Vertrages

(1) Dieser Datenverarbeitungsvertrag (nachstehend "Vertrag" genannt) gilt für alle Datenverarbeitungstätigkeiten, die der Auftragnehmer für den Auftraggeber im Rahmen der in der Anlage/den Anlagen aufgeführten Dienstleistung(en) durchführt.

(2) Änderungen des Verarbeitungsgegenstandes und des Verfahrens werden zwischen dem Auftraggeber und dem Auftragnehmer gemeinsam vereinbart und schriftlich oder in einem dokumentierten elektronischen Format festgehalten.

(3) Dieser Vertrag gilt auf unbestimmte Zeit und bleibt so lange in Kraft, bis der letzte Dienstleistungsvertrag abgelaufen ist oder eine der Parteien ihn unter Einhaltung einer Frist von 30 Tagen schriftlich kündigt. Dieser Vertrag kann von jeder Partei mit sofortiger Wirkung gekündigt werden, wenn die andere Partei die Bestimmungen des Vertrags wesentlich verletzt hat und diese Verletzung nicht innerhalb von 15 Tagen behoben wird.

§ 3 Einzelheiten der Datenverarbeitung

(1) Die Art und der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers sind in der/den jeweiligen Dienstleistungsvereinbarung(en) und insbesondere in Anlage 1 zu diesem Vertrag beschrieben. Der Auftragnehmer ist verpflichtet, den Gegenstand des Dienstleistungsvertrages gemäß den Bestimmungen dieses Vertrages zu erfüllen und alle erforderlichen Verarbeitungsschritte durchzuführen.

(2) Die Arten der betroffenen Daten und die Kategorien der von der Verarbeitung betroffenen Personen sind in Anhang 1 zu diesem Vertrag beschrieben.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur in dem Umfang, der für die Erfüllung des Dienstleistungsvertrags/der Dienstleistungsvereinbarungen erforderlich ist, in Übereinstimmung mit diesem Vertrag und dem geltenden Recht.

(2) Der Auftragnehmer unterlässt jede Nutzung und Verarbeitung zu privaten, persönlichen oder sonstigen kommerziellen oder geschäftlichen Zwecken. Der Auftragnehmer wird den Zugriff auf die Daten des Auftraggebers so weit wie möglich vermeiden. Ist ein Datenzugriff erforderlich, so ist der Auftraggeber verpflichtet, diesen auf das für die konkrete Auftragserfüllung mögliche Minimum zu beschränken.

(3) Der Auftragnehmer ist verpflichtet, mit der erforderlichen Sorgfalt dafür Sorge zu tragen, dass alle mit der Datenverarbeitung betrauten Personen die gesetzlichen Datenschutzbestimmungen einhalten, Daten ausschließlich nach den Weisungen des Auftraggebers verarbeiten und die vom Auftraggeber erhaltenen Daten nicht an Dritte weitergeben oder in sonstiger Weise abweichend verwenden. Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung betrauten Personen auf das Datengeheimnis verpflichtet sind.

(4) Der Auftragnehmer hat alle nach Artikel 32 DSGVO erforderlichen Maßnahmen zu treffen. Weitere Einzelheiten sind in § 8 dieses Vertrages (Technische und organisatorische Maßnahmen) sowie in Anlage 2 geregelt.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Kenntnis von einer Verletzung des Schutzes der für den Auftraggeber verarbeiteten personenbezogenen Daten erhält (z.B. unberechtigter Zugriff). Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Meldepflichten nach dem geltenden Recht.

(6) Die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers lauten data-privacy-solutions-GLOBAL@nttdata.com.

(7) Bei schwerwiegenden Störungen des Betriebsablaufs, die zu Risiken für die personenbezogenen Daten des Auftraggebers führen, bei begründetem Verdacht auf Datenschutzverletzungen oder bei sonstigen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers wird der Auftragnehmer den Auftraggeber unverzüglich informieren. Gleiches gilt, wenn der Auftragnehmer der Auffassung ist, dass die zwischen den Parteien vereinbarten Sicherheitsmaßnahmen nicht mehr den geltenden gesetzlichen Anforderungen entsprechen. Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, alle Verletzungen des Schutzes personenbezogener Daten umfassend zu dokumentieren und ggf. unverzüglich den Aufsichtsbehörden und den Betroffenen zu melden. Der Auftragnehmer unterrichtet den Auftraggeber auch über die Kontrollhandlungen und -maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag bzw. die damit verbundenen Datenverarbeitungen beziehen. Dies gilt auch, wenn eine zuständige Behörde die Datenverarbeitung beim Auftragnehmer im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens untersucht.

In einem solchen Fall können die Parteien eine Unterbrechung der Verarbeitungstätigkeit vereinbaren. Der Auftragnehmer unterrichtet den Auftraggeber über eine solche Unterbrechung der Verarbeitungstätigkeit. Der Auftragnehmer unterrichtet den Auftraggeber über das spätere Ergebnis einer Kontrolle durch die Aufsichtsbehörden oder anderer zuständige Behörden im Zusammenhang

mit diesem Vertrag. Der Auftragnehmer behebt die festgestellten Mängel unverzüglich und ergreift geeignete Maßnahmen zur Beseitigung dieser Mängel.

(8) Sind personenbezogene Daten oder personenbezogene Datenspeicher des Auftraggebers durch Pfändung, Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder sonstige Ereignisse oder Maßnahmen Dritter gefährdet, wird der Auftragnehmer den Auftraggeber unverzüglich über diese Umstände unterrichten.

(9) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

§ 5 Verantwortlichkeiten des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts verantwortlich, insbesondere für die Rechtmäßigkeit der Datenübermittlung an den Auftragnehmer und der Datenverarbeitung. Darüber hinaus ist der Auftraggeber als Verantwortlicher für die personenbezogenen Daten allein für die Wahrung der Rechte der betroffenen Personen gemäß Artikel 12 bis 22 DSGVO verantwortlich ("Verantwortlicher" im Sinne von Artikel 4 Nr. 7 DSGVO).

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und umfassend über Fehler oder Unregelmäßigkeiten in den Verarbeitungsergebnissen oder Datenschutzbestimmungen zu informieren oder wenn er, gleich aus welchem Grund, nicht mehr berechtigt ist, die personenbezogenen Daten an den Auftragnehmer weiterzugeben. Diese Informationspflicht besteht ferner, wenn er Kontrollhandlungen und -maßnahmen der zuständigen Aufsichts- oder Fachbehörden im Rahmen einer Ordnungswidrigkeit, eines Strafverfahrens oder von Haftungsansprüchen einer betroffenen Person oder eines Dritten ausgesetzt ist, soweit sich diese Umstände auf diesen Vertrag beziehen oder auswirken können. Im Hinblick auf eine Unterbrechung der Datenverarbeitung gelten die Regelungen des § 4 (8) dieses Vertrages.

(3) Wird der Auftraggeber von einer betroffenen Person im Hinblick auf eines der in Artikel 82 DSGVO definierten Rechte in Anspruch genommen, so ist der Auftraggeber selbst für die Abwehr dieses Anspruchs verantwortlich. Der Auftragnehmer kann den Auftraggeber in dieser Angelegenheit durch eine besondere Vereinbarung unterstützen.

(4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Geschäftsgeheimnisse und Datensicherungsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 6 Weisungsrechte des Auftraggebers

(1) Der Auftragnehmer wird die ihm gemäß den Bestimmungen in § 4 dieses Vertrages zur Verfügung gestellten Daten nur nach dokumentierten Weisungen des Auftraggebers und im Rahmen der

geschlossenen Vereinbarungen verarbeiten. Der Auftraggeber hat das Recht und die Pflicht, Weisungen über Art, Umfang und Verfahren der Verarbeitungstätigkeiten in Bezug auf die vom Auftragnehmer erbrachte(n) Dienstleistung(en) zu erteilen.

(2) Die Weisungen ergeben sich zunächst aus diesem Vertrag und den/den entsprechenden Dienstleistungsvertrag(en) gemäß § 2 (1) dieses Vertrages. Sie können nachträglich vom Auftraggeber durch Einzelanweisungen oder in einem vereinbarten elektronischen Format (z.B. Ticketsystem, Fax oder E-Mail) an den Auftragnehmer geändert, ergänzt und / oder ersetzt werden. Nicht im Vertrag vorgesehene Weisungen oder Aufträge gelten als Änderungswunsch für die Ausführung der Leistung(en), für den eine entsprechende Änderungsvereinbarung in schriftlicher Form erforderlich ist. Mündliche Weisungen sind unverzüglich schriftlich oder in dokumentierter elektronischer Form zu bestätigen; der Auftragnehmer ist berechtigt, die Ausführung einer Weisung bis zu deren Bestätigung auszusetzen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis ihre Rechtmäßigkeit vom Auftraggeber bestätigt wird oder sie zu einer rechtlich zulässigen Weisung wird.

§ 7 Datenverarbeitung außerhalb der EU/EWR

(1) Soweit im Einzelfall relevant, kann die Verarbeitung durch den Auftragnehmer in einem Drittland außerhalb der EU/ des EWR oder der Schweiz durchgeführt werden.

(2) Die Erbringung von vertraglich vereinbarten Datenbearbeitungen außerhalb der EU/ des EWR oder der Schweiz, insbesondere die Übermittlung von Daten in oder aus einem Drittstaat sowie die Übermittlung von Personendaten, erfolgt unter Einhaltung der Anforderungen gemäß Art. 44 ff. GDPR. :

- wenn der Empfänger, das Land oder das Gebiet, in dem personenbezogene Daten verarbeitet oder abgerufen werden, ein angemessenes Schutzniveau für die Rechte und Freiheiten der betroffenen Personen im Hinblick auf die Verarbeitung personenbezogener Daten gewährleistet, wie es von der Europäischen Kommission festgelegt wurde; oder
- wenn mit den jeweiligen Empfängern oder Ländern Standardvertragsklauseln (SCCs auf der Grundlage von Schrems II) vereinbart wurden.

(3) Die EU-Standardvertragsklauseln (Fassung 2021 auf der Grundlage des Schrems-II-Urteils des Europäischen Gerichtshofs) müssen vom Auftragnehmer angewandt werden, wenn eine internationale Übermittlung in ein Land erfolgt, das kein angemessenes Schutzniveau für die Rechte und Freiheiten der betroffenen Personen in Bezug auf die Verarbeitung personenbezogener Daten gewährleistet, wie von der Europäischen Kommission festgelegt.

(4) Im Falle von Unterauftragsverarbeitern aus Drittländern muss der Auftragnehmer sicherstellen, dass diese ein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten bieten. Der

Auftragnehmer muss von seinen Unterauftragsverarbeitern verlangen, dass sie vor der Verarbeitung personenbezogener Daten durch den Unterauftragsverarbeiter Datenverarbeitungsverträge und/oder Standardvertragsklauseln abschließen, sobald dies erforderlich ist. Diese Verträge müssen der/den Datenverarbeitungsvereinbarung(en) zwischen dem Auftragnehmer und dem Auftraggeber entsprechen und ein ähnliches Datenschutzniveau gewährleisten. Der Auftragnehmer setzt die Standardvertragsklauseln (Fassung 2021 auf der Grundlage der Schrems-II-Entscheidung des Europäischen Gerichtshofs) gegenüber dem Unterauftragsverarbeiter im Namen des für die Verarbeitung Verantwortlichen durch, wenn kein direktes datenschutzrechtliches Durchsetzungsrecht zur Verfügung steht, wozu der Auftragnehmer hiermit vom Auftraggeber ausdrücklich ermächtigt wird.

§ 8 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die interne Organisation in seinem Verantwortungsbereich so zu gestalten, dass die spezifischen Anforderungen der einschlägigen Datenschutzbestimmungen eingehalten und geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten, das dem aktuellen Stand der Technik für die jeweiligen Verarbeitungstätigkeiten entspricht und die Anforderungen des Artikels 32 DSGVO erfüllt.

(2) Der Auftraggeber prüft die dokumentierten technischen und organisatorischen Maßnahmen des Auftragnehmers (Anlage 2) im Rahmen einer Vorprüfung vor Beginn der Datenverarbeitung durch den Auftragnehmer. Erforderliche Anpassungen dieser Maßnahmen unter Berücksichtigung des mit der jeweiligen Verarbeitungstätigkeit verbundenen Risikos werden dem Auftragnehmer vom Auftraggeber mitgeteilt und im gegenseitigen Einvernehmen zwischen den Parteien durch Anpassung der vorgelegten technischen und organisatorischen Maßnahmen (Anlage 2) beschlossen.

(3) Die vereinbarten Maßnahmen sind in Anlage 2 zu diesem Vertrag dokumentiert. Der Auftraggeber hat Kenntnis von diesen technischen und organisatorischen Maßnahmen und ist dafür verantwortlich, dass sie ein Sicherheitsniveau gewährleisten, das den Risiken für die Rechte und Freiheiten einer natürlichen Person, hinsichtlich der vom Auftragnehmer zu verarbeitenden Daten, angemessen ist.

(4) Der Auftragnehmer behält sich das Recht vor, die technischen und organisatorischen Maßnahmen von Zeit zu Zeit anzupassen, muss jedoch sicherstellen, dass das für die Verarbeitung gebotene Schutzniveau nicht unter das angemessene Mindestsicherheitsniveau zur Einhaltung von Artikel 35 DSGVO fällt. Der Auftragnehmer informiert den Auftraggeber über alle wesentlichen Änderungen der technischen und organisatorischen Maßnahmen (Anhang 2).

(5) Der Auftragnehmer überwacht regelmäßig seine internen Prozesse und technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung der personenbezogenen Daten des Auftraggebers in Übereinstimmung mit den Anforderungen des geltenden Datenschutzrechts (insbesondere Artikel 32 der DSGVO) erfolgt. Der Auftragnehmer weist dem Auftraggeber auf dessen

begründetes Verlangen in geeigneter Weise nach, dass er die in diesem Vertrag festgelegten Verpflichtungen und Maßnahmen einhält.

§ 9 Rechte der betroffenen Personen

(1) Die Rechte der betroffenen Personen, die sich aus der Erhebung, Verarbeitung und Nutzung ihrer Daten durch den Auftragnehmer ergeben, sind stets gegenüber dem Auftraggeber geltend zu machen. Der Auftraggeber ist für die Wahrung dieser Rechte verantwortlich. Insbesondere obliegt dem Auftraggeber die Benachrichtigung der Betroffenen, die Erteilung von Auskünften, die Sicherstellung der Berichtigung, Löschung und Sperrung von personenbezogenen Daten. Der Auftraggeber informiert den Auftragnehmer unverzüglich über die notwendigen Aktivitäten zur Wahrnehmung dieser Rechte der betroffenen Personen.

(2) Wendet sich eine betroffene Person direkt an den Auftragnehmer, so leitet der Auftragnehmer diese Anfrage unverzüglich an den Auftraggeber weiter und verweist die betroffene Person an den Auftraggeber, sofern es möglich ist, die Anfrage auf der Grundlage der von der betroffenen Person bereitgestellten Informationen mit dem Auftraggeber in Verbindung zu bringen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung und Erfüllung von Anfragen der betroffenen Personen. Ist der Auftraggeber beispielsweise nach geltendem Datenschutzrecht verpflichtet, einer betroffenen Person Auskunft über die Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten zu erteilen, stellt der Auftragnehmer dem Auftraggeber auf Anfrage die hierfür erforderlichen Informationen im Rahmen des Möglichen zur Verfügung.

(4) Der Auftragnehmer ist nicht berechtigt, die im Auftrag des Auftraggebers verarbeiteten personenbezogenen Daten zu berichtigen, zu löschen oder einzuschränken; derartige Maßnahmen des Auftragnehmers sind nur nach dokumentierten Anweisungen des Auftraggebers zulässig.

§ 10 Prüfungsrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die technischen und organisatorischen Maßnahmen des Auftragnehmers vor Beginn der Verarbeitung und danach durch Einholung von Auskünften des Auftragnehmers, Anforderung bestimmter zumutbarer Nachweise beim Auftragnehmer oder durch Selbstauskünfte des Auftragnehmers in geeigneter Weise zu kontrollieren. Der Nachweis kann beispielsweise durch die folgenden Arten von Informationen erbracht werden:

- Protokoll eines erfolgten Selbstaudits (aktuelle Bescheinigungen, Berichte oder Berichtsauszüge unabhängiger Stellen (z.B. Datenschutzbeauftragte, Auditoren, IT-Sicherheitsabteilung, Datenschutzauditoren).
- Dokumentationsnachweise unternehmensinterner Verhaltensregeln/Verfahren, einschließlich des Nachweises der Einhaltung dieser Regeln.
- Zertifikat für Informationssicherheit (z. B. ISO 27001).

- Nachweis einer entsprechenden Zertifizierung nach einem IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(2) Der Auftraggeber und der Auftragnehmer können vereinbaren, dass der Nachweis auch durch andere Dokumente / Bescheinigungen erbracht werden kann.

(3) Führen die Kontrollmaßnahmen nach § 10 (1) dieses Vertrages nicht zu Klarheit für den Auftraggeber, wird ein Audit durch den Auftraggeber oder einem von ihm beauftragten Wirtschaftsprüfer zwischen den Parteien vereinbart.

(4) Soweit im Einzelfall Kontrollen am Sitz des Auftragnehmers durch den Auftraggeber oder einen im Auftrag des Auftraggebers handelnden externen Prüfer erforderlich sind, können diese durch den Datenschutzbeauftragten des Auftraggebers und andere vom Auftraggeber beauftragte Stellen nach rechtzeitiger Unterrichtung des Datenschutzbeauftragten des Auftragnehmers durchgeführt werden, dass die Maßnahmen zur Einhaltung der technischen und organisatorischen Anforderungen der einschlägigen Datenschutzgesetze für die Verarbeitung durch den Auftragnehmer geeignet sind. Das Audit findet in den Räumen des Auftragnehmers während der üblichen Geschäftszeiten ohne Störung des Betriebs statt. Der Auftragnehmer kann Audits von der vorherigen Unterzeichnung einer Vertraulichkeitsvereinbarung über das einzelne Audit abhängig machen, z.B. in Bezug auf die Daten anderer Kunden.

(5) Beauftragt der Auftraggeber einen Dritten mit der Prüfung, so hat er diesen ebenfalls schriftlich zur Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, der Dritte unterliegt einer beruflichen Schweigepflicht. Steht der Prüfer des Auftraggebers in einem Wettbewerbsverhältnis zum Auftragnehmer, hat der Auftragnehmer das Recht, einen anderen Prüfer zu verlangen.

§ 11 Unterauftragnehmer

(1) Unter Unterauftrags-Geschäftsbeziehungen im Sinne dieser Bestimmung sind Leistungen zu verstehen, die von Unterauftragnehmern (weiteren Datenverarbeitern) erbracht werden und die sich unmittelbar auf die Erbringung der Leistung(en) aus dieser Datenverarbeitungsvereinbarung und den damit verbundenen Dienstleistungsvertrag(en) beziehen. Nicht als Unterauftragsverhältnisse definiert sind zusätzliche, vom Auftragnehmer in Anspruch genommene Nebenleistungen, z.B. in Form von Telekommunikationsleistungen, Post-/Transportleistungen, Wartungs- und Benutzungsleistungen und/oder die Entsorgung von Datenträgern oder Dokumenten sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungssystemen. Der Auftragnehmer ist jedoch verpflichtet, auch bei solchen ausgelagerten Nebenleistungen angemessene und rechtskonforme vertragliche Regelungen und Kontrollmaßnahmen zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers zu treffen.

(2) Der Auftragnehmer kann Unterauftragnehmer wie verbundene Unternehmen oder externe Dienstleister mit der Verarbeitung personenbezogener Daten des Auftraggebers beauftragen. Hat der

Auftraggeber berechtigte Bedenken hinsichtlich eines ausgewählten Unterauftragnehmers, kann der Kunde dem ausgewählten Unterauftragnehmer widersprechen.

(3) Der Auftragnehmer muss mit den an der Datenverarbeitung beteiligten Unterauftragnehmern Verträge abschließen. In diesen Verträgen werden dem Unterauftragnehmer Vertraulichkeits-, Datenschutz- und Datensicherheitsverpflichtungen auferlegt, die dem durch diesen Vertrag gebotenen Datenschutz- und Sicherheitsniveau entsprechen und dieses Niveau nicht unterschreiten. Der Auftragnehmer muss regelmäßig (unter Berücksichtigung des risikobasierten Ansatzes) überprüfen, ob die eingesetzten Unterauftragnehmer diese vertraglichen Verpflichtungen einhalten. Der Auftraggeber ist jederzeit berechtigt, vom Auftragnehmer auf schriftliche Anfrage eine Übersicht der für die Dienstleistung eingesetzten Unterauftragnehmer sowie Informationen über den Inhalt der Verträge, der Umsetzung der Datenschutzverpflichtungen der Unterauftragnehmer sowie Nachweise der Überprüfung der eingesetzten Unterauftragnehmer durch den Auftragnehmer zu erhalten.

(4) Jegliche Datenübermittlung an einen Unterauftragnehmer des Auftragnehmers darf erst beginnen, wenn der Unterauftragnehmer alle mit dieser Vereinbarung vergleichbaren Anforderungen erfüllt.

(5) Erbringt der Unterauftragnehmer die vereinbarte Dienstleistung außerhalb der EU/des EWR, ergreift der Auftragnehmer alle erforderlichen Maßnahmen, um sicherzustellen, dass die Verarbeitung im Einklang mit den Anforderungen der EU-DSGVO, insbesondere mit Artikel 46 (2) c) (Standardvertragsklauseln), erfolgt. Abschnitt 7 dieses Vertrags ist entsprechend anwendbar.

§ 12 Löschung und Rückgabe von personenbezogenen Daten

(1) Nach Vertragsbeendigung oder zu jedem anderen Zeitpunkt wird der Auftragnehmer die vom Auftraggeber überlassenen personenbezogenen Daten, die für den Auftraggeber erhobenen, verarbeiteten und/oder genutzten personenbezogenen Daten, die vom Auftraggeber erstellten Verarbeitungs- und Nutzungsergebnisse sowie etwaige Kopien davon und die vom Auftraggeber im Zusammenhang mit dem Vertragsverhältnis erhaltenen Unterlagen nach Wahl des Auftraggebers löschen, vernichten oder an den Auftraggeber zurückgeben. Ist die Offenlegung oder Rückgabe der Daten oder etwaiger Kopien davon aus technischen Gründen nicht möglich (z.B. wegen elektronischer Speicherung auf fest installierten oder - soweit datenschutzrechtlich zulässig - gemeinsam genutzten Medien) oder wird vom Auftraggeber eine Löschung/Vernichtung verlangt, werden die entsprechenden Daten vom Auftragnehmer in Absprache mit dem Auftraggeber und unter Beachtung der Datenschutzgesetze gelöscht.

(2) Elektronisch gespeicherte Daten werden auf Verlangen des Auftraggebers entweder in handelsüblicher Form auf elektronischen Datenträgern bereitgestellt oder online übertragen. Dies gilt nicht für Sicherungskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, und für Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten benötigt werden. Der Auftragnehmer kann diese dem Auftraggeber bei Vertragsende zur Entlastung des Auftragnehmers zugänglich machen.

(3) Der Auftragnehmer wird dem Auftraggeber die Löschung/Vernichtung elektronisch-gespeicherter Daten / von Datenträgern schriftlich oder per E-Mail bestätigen. Weitergehende gesetzliche Löschungspflichten und Löschungsansprüche bleiben von den vorstehenden Regelungen unberührt.

§ 13 Schlussbestimmungen

(1) Die nachstehend aufgeführten Anhänge sind Bestandteil dieses Vertrags. Änderungen oder Ergänzungen dieses Vertrages oder eines seiner Bestandteile bedürfen der Schriftform, soweit nicht ausdrücklich etwas anderes vereinbart ist. Dies gilt auch für einen Verzicht auf dieses Formerfordernis. Zusätzliche Nebenabreden haben die Parteien nicht getroffen.

(2) Der Vertrag, Vertragsänderungen und künftige Nebenabreden bedürfen der Schriftform; dies kann auch auf elektronischem Wege geschehen. Mitteilungen/Informationen, Zustimmungserklärungen, Genehmigungserklärungen und Bestätigungen können per E-Mail übermittelt werden.

(3) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder durch eine nach Vertragsschluss eingetretene Änderung der Rechtslage unwirksam oder undurchführbar werden, so wird hierdurch die Gültigkeit des Vertrages im Übrigen nicht berührt. Die unwirksame oder undurchführbare Bestimmung ist durch eine wirksame und durchführbare Bestimmung zu ersetzen, die dem mit der unwirksamen Bestimmung verfolgten Zweck möglichst nahekommt. Die Parteien werden eine entsprechende Regelung treffen, die diesem Ziel gerecht wird.

Liste der Anhänge

Anhang 1: Datenverarbeitungstätigkeiten, Art und Zweck, Arten von Daten und betroffene Personen

Anhang 2: Technische und organisatorische Maßnahmen

§ 14 Unterschriften

Auftraggeber

Customer Name
[Firmenadresse]
Datum:

Auftragnehmer

NTT DATA Business Solutions AG
Bielefeld
Datum:

Unterschrift	Unterschrift	Unterschrift	Unterschrift
Name in Druckbuchstaben	Name in Druckbuchstaben	Name in Druckbuchstaben	Name in Druckbuchstaben
Titel/Funktion	Titel/Funktion	Titel/Funktion	Titel/Funktion
Stempel		Stempel	

Anhang 1: Wartung

(1) Beschreibung der Dienstleistung

NTT DATA Business Solutions erbringt Software-Pflegeleistungen und die Bereitstellung von Enterprise Supportleistungen an die, in dem Lizenz- und Pflegevertrag erworbene, SAP Standardsoftware. Der Umfang der Wartungsleistungen ist in Ziffer 3 "Leistungsumfang der Softwarepflege" sowie in der "Leistungsbeschreibung NTT DATA-Software-Pflege – NTT DATA Enterprise Support" aufgeführt.

2) Betroffene Personen

- Kunden (Mitarbeiter des Kunden sowie mögliche Endkunden, die von der Nutzung des Dienstes durch den Kunden betroffen sind)
- Lieferanten
- Dienstleister (z. B. externe Berater, externe Ausbilder)
- Strategische Partner
- Weitere:

(3) Arten von Daten.

Die für die Erbringung des Dienstes verarbeiteten Datenarten sind:

- Personenbezogene Stammdaten/Personenidentifikationsdaten (z.B. Name, Adresse, Berufsbezeichnung, Unternehmenszugehörigkeit)
- Elektronische Identifizierungsdaten (z. B. IP-Adresse, elektronische Signatur, Verbindungs-/Log-Daten, Cookies)
- Kommunikationsdaten (z.B. Telefon, E-Mail, PIN, Passwort, Ports, Login)
- Weitere:

(4) Häufigkeit der Übermittlung

Personenbezogene Daten können während der gesamten Vertragslaufzeit der Dienstleistung(en) übermittelt werden.

(5) Löschfristen

Personenbezogene Daten können für die Dauer des Dienstleistungsvertrags gespeichert werden.

Anhang 2: Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der übermittelten personenbezogenen Daten

1. Vertraulichkeit

Zu den Maßnahmen zur Umsetzung der Vertraulichkeitsanforderung gehören u.a. Maßnahmen zur Zutritts-, Zugangs- oder Zugriffskontrolle. In diesem Zusammenhang sollen die folgenden technischen und organisatorischen Maßnahmen seitens des Auftragnehmers ein angemessenes Sicherheitsniveau für personenbezogene Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder missbräuchlicher Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Beschädigung.

a.) Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zugang zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet und genutzt werden.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Absicherung von Gebäudeschächten
- Einbruchmeldeanlage
- Videoüberwachung an den Eingängen
- Sicherheitstüren und -schlösser
- Lichtschranken/Bewegungsmelder
- Manuelles Schließsystem
- Verschluss-System mit codierten Schlössern
- Automatisches Zutrittskontrollsystem
- Chipkarten/Transponder-Schließsystem
- Schlüsselliste
- Biometrische Zutrittskontrollen zu den Serverräumen in unseren Rechenzentren
- Unterteilung in verschiedene Sicherheitszonen
- Funktions- und rollenbasierte Zutrittsberechtigungen
- Die Bewachung des Geländes/Gebäudes außerhalb der Geschäftszeiten sowie an Wochenenden und Feiertagen erfolgt durch einen externen Sicherheitsdienst.
- 7x24h Wachschutz in den Rechenzentren
- Einsatz von sorgfältig ausgewähltem Sicherheitspersonal
- Sorgfältige Auswahl des Reinigungspersonals
- Pflicht zum Mitführen von Zutrittskarten
- Identitätskontrollen durch Wachschutz (nur in unseren Rechenzentren) / Empfangspersonal
- Protokollierung der Besucher

b.) Zugangskontrolle

Maßnahmen zur Verhinderung der Nutzung von Datenverarbeitungssystemen durch Unbefugte.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- 2-Faktor-Authentifizierung
- Authentifizierung über Benutzernamen/Passwort
- Passwortkontrolle (Mindestlänge, Komplexität, Gültigkeitsdauer, Sperren usw.)
- Verwendung von Antiviren-Software
- Verwendung einer Hardware-Firewall
- Verwendung einer Software-Firewall
- Verwendung von Aktenvernichtern
- Sichere Aufbewahrung von Datenträgern (Backup-Bänder, Festplatten usw.)
- Verschlüsselung auf Verzeichnis- und Dateiebene
- Einsatz eines Identitätsmanagementsystems
- Verschlüsselung von Datenträgern in Laptops/Notebooks
- Verschlüsselung von Smartphone-Inhalten
- Einsatz der VPN-Technologie
- Verschlüsselung von mobilen Datenträgern (Festplatten, USB-Sticks, SD-Karten, usw.)
- Verwendung von sicheren Transportbehältern/Verpackungen für den physischen Transport *
- Sorgfältige Auswahl von Transportpersonal und Fahrzeugen*
- Verwendung von abschließbaren Entsorgungsbehältern für Papier, Akten und Datenträger
- Vernichtung von Datenträgern durch zertifizierte Entsorgungsunternehmen
- Vernichtung von Papierdokumenten durch zertifizierte Entsorgungsunternehmen
- Erstellung von Benutzerprofilen (funktions- und rollenbasiert)
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Netzwerk- und Netzwerkzonenkonzept
- Notfallmanagement für Auftraggeber (z.B. Mehrschichtbetrieb, Bereitschaftsdienst, Vertretungsregelung)*

Die mit * gekennzeichneten Maßnahmen sind serviceabhängig und bedürfen einer individuellen, schriftlichen Beauftragung durch den Auftraggeber.

c.) Zugriffskontrolle

Maßnahmen, die sicherstellen, dass nur die Berechtigten zur Nutzung eines Datenverarbeitungssystems auf die Daten zugreifen können und dass personenbezogene Daten während der Verarbeitung und Nutzung oder nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Anzahl der Administratoren sind auf ein Minimum beschränkt
- Protokollierung von Zugriffen auf Applikationen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Funktions- und rollenbasiertes Berechtigungskonzept

- Verwaltung der Zugangsberechtigungen unter Beachtung der Funktionstrennung und des Vier-Augen-Prinzips
- Aufzeichnungen über die Vernichtung von Papier, Akten und Datenträgern

d.) Trennungskontrolle

Maßnahmen, die sicherstellen, dass für unterschiedliche Zwecke erhobene Daten getrennt verarbeitet werden können.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Für pseudonymisierte Daten: Trennung der Zuordnungsdatei und Speicherung auf einem separaten, sicheren IT-System
- Physisch getrennte Speicherung auf separaten Systemen oder Datenträgern
- Festlegung von Datenbankrechten
- Versehen der Datensätze mit Zweckattributen
- Logische Client-Trennung (software-seitig)
- Trennung von Produktiv-, Test- und Entwicklungssystemen

e.) Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen getrennt aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Das Pseudonymisierungsgebot ist ein zentraler Bestandteil des Datenschutzkonzeptes des Auftragnehmers
- Sichere Speicherung der für die Pseudonymisierung verwendeten kryptografischen Schlüssel
- Berechtigungskonzept für den Zugriff auf kryptografische Schlüssel, die eine Personalisierung ermöglichen
- Die Pseudonymisierung der Daten des Auftraggebers erfolgt nur auf Anweisung und in Absprache mit dem Auftraggeber.

f.) Verschlüsselung (Encryption)

Die Verschlüsselung dient dazu, den Zugriff auf personenbezogene Daten durch Unbefugte zu verhindern oder vor diesen zu warnen (z. B. vor Hackerangriffen oder Spionage). Verschlüsselung bezeichnet den Prozess der Umwandlung von Daten in eine Form, die als Chiffretext bezeichnet wird und für Unbefugte schwer zu verstehen ist.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Verwendung einer dem Informationssicherheitskonzeptes entsprechenden Verschlüsselungsmethode

- Auswahl eines geeigneten Verfahrens zur Verschlüsselung nach dem neuesten Stand der Technik
- Regelmäßige Überprüfung der Verschlüsselungsmethoden auf Sicherheitslücken und ggf. Aktualisierung der entsprechenden Software
- E-Mail-Verschlüsselung
- Verschlüsselung auf Verzeichnis- und Dateiebene
- Prozesse zur Verwaltung und zum Schutz kryptographischer Informationen (Berechtigungskonzept für interne und externe Mitarbeiter)
- Verschlüsselung von Smart Devices
- Verschlüsselung von Massenspeichern in Laptops und Notebooks
- Verschlüsselung von mobilen Datenträgern (Festplatten, USB-Sticks, SD-Karten, usw.)
- Die Verschlüsselung der Daten des Auftraggebers erfolgt nur auf Anweisung und in Absprache mit dem Auftraggeber.

2. Integrität

Zu den Maßnahmen zur Umsetzung des Integritätsgebots gehören zum einen solche im Rahmen der Eingabekontrolle, zum anderen aber auch solche, die allgemein dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Beschädigung dienen. In diesem Zusammenhang sollen die folgenden technischen und organisatorischen Maßnahmen des Auftragnehmers die Integrität der personenbezogenen Daten sicherstellen.

a.) Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übermittlung, beim Transport oder bei der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass die vorgesehenen Empfänger, der mit Hilfe von Datenübertragungseinrichtungen übermittelten Daten, überprüft und ermittelt werden können.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Verpflichtung der Mitarbeiter zum Verbot des Verrats von Geschäfts- und Betriebsgeheimnissen
- Verpflichtung der Mitarbeiter auf das Datengeheimnis in Übereinstimmung mit den lokal geltenden Datenschutzgesetzen
- Einrichtung von Standleitungen oder VPN-Tunneln
- E-Mail-Verschlüsselung
- Dokumentation der Datenempfänger bzw. der vereinbarten Löschungsfristen
- Übermittlung von Daten in anonymer oder pseudonymisierter Form (nach Weisung des Auftraggebers)

Die Weitergabe der Daten des Auftraggebers erfolgt nur im Einvernehmen mit dem Auftraggeber.

b.) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Aufbewahrung von Formularen, aus denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Protokollierung der Eingabe, Änderung und Löschung von Daten (Logging)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts
- Erstellung einer Übersicht, aus der hervorgeht, mit welchen Anwendungen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch einzelne Benutzernamen (nicht Benutzergruppen)
- Die Mitarbeiter des Auftragnehmers erstellen, ändern oder löschen Daten oder Datensätze des Auftraggebers nur nach individueller, schriftlicher Anweisung und im Rahmen des Incident- und Change-Managements gemäß ISO/IEC 20000-1:2018. Dabei werden sowohl die Freigabe des Auftraggebers als auch die vorgenommenen Änderungen dokumentiert. Eine Übersicht über die vorgenommenen Änderungen kann auf Anfrage durch den Auftragnehmer bereitgestellt werden.

3. Verfügbarkeit und Widerstandsfähigkeit der Systeme

Maßnahmen, welche gewährleisten, dass Daten und IT-Systeme zur Verfügung stehen und von autorisierten Personen genutzt werden können, wenn dies benötigt wird. Eine unbefugte Unterbrechung z.B. durch Serverausfall oder Ausfall von Kommunikationsmitteln stellt einen Angriff auf die Verfügbarkeit dar. Durch diese Maßnahmen soll auch sichergestellt werden, dass die Systeme, auf denen personenbezogene Daten gespeichert sind, einer gewissen Belastung standhalten können, regelmäßig überwacht werden, sowie ein entsprechendes Notfallmanagement eingerichtet ist.

a.) Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Notfallhandbuch
- Notfallplan
- Brand- und Rauchmeldeanlagen
- Regelungen zur Verfügbarkeit und Zuverlässigkeit der Leistung des Auftragnehmers
- Tests zur Datenwiederherstellung*
- Konzept für die Sicherung und Wiederherstellung von Daten (Backup, Restore, Recovery)
- Aufbewahrung von Datensicherungen an einem sicheren und ausgelagerten Ort

- Konzept zur Archivierung der Daten
- Einzelheiten zu der zwischen Auftraggeber und Auftragnehmer vereinbarten Verfügbarkeit sowie den Backup-, Restore- und Recovery-Maßnahmen sind im zugrundeliegenden Dienstleistungsvertrag beschrieben.

Zusätzliche technische Maßnahmen in unseren Rechenzentren:

- Brand- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen
- Feuerlöschanlagen in Serverräumen
- Überspannungsschutzkonzept in Serverräumen
- Klimatisierte Serverräume
- Geräte zur Überwachung von Temperatur und Luftfeuchtigkeit in Serverräumen
- Maßnahmen zur Verhinderung von Wassereinbrüchen in Serverräumen
- Kühltechnik in Racks
- Unterbrechungsfreie Stromversorgung (UPS)
- Redundante Serverräume

b.) Ausfallsicherheit der Systeme und Dienste

Dazu gehören Maßnahmen, die der Auftragnehmer zur Überwachung der Systeme und zur frühzeitigen Erkennung und Vermeidung von starker Systembelastung einsetzt.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Überwachung der Systeme auf Angriffe
- Penetrationstests
- Einstellung und Überwachung der Belastungsgrenze für die jeweiligen Systeme (Capacity Management)
- Schwachstellen- und Patchmanagement
- Für weitere Details siehe 4 a) "Verfügbarkeitskontrolle"

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a.) Organisatorische Kontrolle

Maßnahmen zur Gestaltung der internen Organisation, die den besonderen Anforderungen des Datenschutzes gerecht werden.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Datenschutz-Management-System
- Tätigkeitsbeschreibungen der Mitarbeiter in Stellen-, Funktions- und Rollenbeschreibungen
- Meldeverfahren
- Management von Datenpannen und Sicherheitsvorfällen
- Auskunfts- und Informationsverfahren
- Entsorgungskonzept
- Trennung von Funktionen und Verantwortung zwischen Dateninhabern und -verarbeitern

- Regelmäßige Datenschutztrainings sowie Informationssicherheitstrainings der Mitarbeiter:innen
- Ernennung eines Datenschutzbeauftragten sowie Festlegung und Bekanntgabe der Aufgaben
- Richtlinien zum Datenschutz und zur Informationssicherheit
- Leitfaden für die zu verwendende Hard- und Software, einschließlich Investitions- und Genehmigungsverfahren
- Erstellung und Pflege eines Verzeichnisses der Verarbeitungstätigkeiten für Auftragsverarbeiter
- Konzept für die Klassifizierung von Informationen, dass eine korrekte und konsistente Klassifizierung von Dokumenten gewährleistet
- Risikomanagement und Informationssicherheit in Projekten
- Risikomanagementprogramm zur Identifizierung, Verwaltung und Weiterverfolgung von Informationssicherheitsrisiken
- Regelmäßige Überprüfung der Richtlinien (mindestens einmal jährlich)
- Bestehendes Programm zur Verwaltung von Schwachstellen, das Schwachstellen identifiziert, verwaltet und verfolgt

b.) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Rahmen des Vertrags verarbeitet werden, nur gemäß den Anweisungen des Kunden verarbeitet werden können.

Die folgenden Maßnahmen werden vom Auftragnehmer durchgeführt:

- Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich der Datensicherheit)
- Überprüfung der Dokumentation und der technischen und organisatorischen Maßnahmen des Auftragnehmers durch den Auftraggeber vor Beginn der Datenverarbeitung
- Regelmäßige Überprüfung der Auftragnehmer
- Abschluss einer Auftragsdatenverarbeitung gemäß Artikel 28 (3) DSGVO
- Schriftliche Weisungen des Auftraggebers an den Auftragnehmer im Rahmen des Servicevertrages
- Vereinbarte wirksame Kontrollrechte des Auftraggebers gegenüber dem Auftragnehmer
- Sicherstellung der Datenvernichtung bzw. Rückgabe der Daten durch den Auftragnehmer an den Auftraggeber nach Beendigung des Auftrags