Anlage 3: Bedingungen der Auftragsverarbeitung

Vorbemerkung

Diese Auftragsverarbeitungsvereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Kunden verarbeiten oder wenigstens Zugriffsmöglichkeit haben.

1. Gegenstand, Dauer, Spezifizierung der Auftragsverarbeitung

(1) Gegenstand der Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen (Kunde) und des Auftragnehmers (Perian), sofern im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten) eine Verarbeitung personenbezogener Daten durch Perian für Kunden im Sinne des anwendbaren Datenschutzrechts erfolgt. Die Vereinbarung gilt entsprechend für die (Fern)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(2) Die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen werden vom Kunden nach alleinigem Ermessen festgelegt und kontrolliert.

(3) Der Auftragnehmer verwendet die zur Kenntnis gelangten personenbezogenen Daten für keine anderen Zwecke als den festgelegten Vertragszweck. Der Auftragnehmer darf die Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach dieser Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Daten im Sinne dieses Vertrags gelten.

(4) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union, in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht sowie UK, USA und Schweiz.

2. Weisungsbefugnisse des Kunden

(1) Weisungsberechtigt auf Seiten des Kunden ist der Kunde selbst, der gesetzliche Vertreter des Kunden und der IT-Leiter. Werden Weisungen durch andere Personen erteilt, müssen diese von den berechtigten Personen bestätigt werden. Mündliche Weisungen bestätigt der Kunde unverzüglich per E-Mail.

(2) Der Auftragnehmer hat den Kunden möglichst zeitnah darauf hinweisen, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

(3) Der Auftragnehmer verwendet die Daten ausschließlich in Übereinstimmung mit den Weisungen des Kunden, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden.

Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers.

3. Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Daten Ansprüche geltend machen, wird der Kunde den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen, wenn der Auftragnehmer dem Kunden nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(2) Der Kunde ist Eigentümer der Daten und Inhaber aller etwaigen Rechte, die die Daten betreffen.

(3) Dem Kunden obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Richtigkeit der Daten. Der Kunde hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Sofern erforderlich, schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten werden auf Anforderung zur Verfügung gestellt.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.

d) Der Kunde und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Kunde seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden im Rahmen seiner Kontrollbefugnisse dieses Vertrages.

5. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Kunden auf Anforderung zur Prüfung zu übergeben. Soweit die Prüfung/ein Audit des Kunden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

6. Mitteilung des Auftragnehmers bei Verstößen

(1) Der Auftragnehmer unterstützt den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Kunden zu melden,

c) die Verpflichtung, dem Kunde im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Kunden für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Kunden im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

7. Kontrollrechte des Kunden

(1) Der Auftragnehmer stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Kunde hat grundsätzlich das Recht, in Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mit 2 Wochen Vorlauf anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer am Ort der Datenverarbeitung zu überzeugen.

(2) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung,

Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts") erbracht werden, wenn der Prüfungsbericht es dem Kunden in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Sofern der Kunde auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht, dass diese Prüfberichte bzw. Zertifizierungen unzureichend oder unzutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung des Kunden dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen.

(3) Dem Kunden ist bekannt, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Verpflichtungen, die in der Anlage 2 benannte Subunternehmer einsetzt. Am Geschäftssitz des Auftragnehmers findet daher lediglich Zugriff auf diese Systeme statt, Ort der Datenverarbeitung ist damit das IT-System des Subunternehmers. Über diese Systeme des Subunternehmers und die Zugriffssysteme des Auftragnehmers verpflichtet sich dieser, dem Kunden auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(4) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Kunden, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Kunde ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten – es sei denn, dass diese die Basis des erstattungsfähigen oder durchlaufenden Aufwandes darstellen – zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

(5) Der Kunde hat den Auftragnehmer rechtzeitig (mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Kunde darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Kunden, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

(6) Der Auftragnehmer erhält vom Kunden eine Aufwandsentschädigung, wenn die Art und Weise einer Kontrolle unverhältnismäßig den Auftragnehmer beeinträchtigt.

(7) Beauftragt der Kunde einen Dritten mit der Durchführung der Kontrolle, hat der Kunde den Dritten schriftlich ebenso zu verpflichten, wie auch der Kunde aufgrund dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Kunde den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Kunde diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Kunde darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

8. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Kunden beauftragen. Der Kunde stimmt der Beauftragung der in der Anlage genannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

(3) Der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Kunden eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Kunde nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 24 DS-GVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Kunden an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die datenschutzrechtlichen Pflichten aus diesem Vertrag sind auf den weiteren Auftragsverarbeiter zu übertragen.

9. Rechte der betroffenen Personen

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Kunden geltend zu machen.

(2) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der sie betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen zeitnah an den Kunden weiterleiten.

(3) Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von Daten oder auf Auskunft über die gespeicherten Daten, den Zweck der Speicherung und die Personen und Orte, an die Daten regelmäßig übermittelt werden, geltend macht, hat der

Auftragnehmer den Kunden bei der Erfüllung dieser Ansprüche in angemessenem und für den Kunden erforderlichen Umfang zu unterstützen, sofern der Kunde die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann. Der Auftragnehmer erhält vom Kunden eine angemessene Entschädigung für seinen im Rahmen der Mitwirkung anfallenden Aufwand.

(4) Der Auftragnehmer wird es dem Kunden ermöglichen, Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Kunden die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Kunde selbst unmöglich ist.

10. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Kunden weiterleiten.

(2) Ein etwaiges Löschkonzept, die Gewährleistung des Rechts auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind unmittelbar durch den Kunden sicherzustellen.

11. Löschung und Rückgabe von personenbezogenen Daten

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Kunden entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach deutschem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt.

12. Verhältnis zum Hauptvertrag

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

13. Aufhebung bisheriger Vereinbarungen

Die Parteien vereinbaren, dass zeitgleich mit Beginn dieser Vereinbarung zur Auftragsverarbeitung mögliche zwischen den Parteien bestehende Vereinbarungen zur Auftragsdatenverarbeitung einvernehmlich aufgehoben und durch diese neue Vereinbarung zur Auftragsverarbeitung ersetzt werden.

14. Verweise auf die DSGVO

Alle in dieser Vereinbarung enthaltenen Verweise auf die DSGVO gelten für die DSGVO in ihrer jeweils aktuellen Fassung bzw. etwaige Nachfolgeregelungen.

Stand Juli 2024