Plusnet
Wir leben Kommunikation

Vereinbarung zur Auftragsdatenverarbeitung

Inhalt

Plusnet
Wir leben Kommunikation

Vereinbarung zur Auftragsdatenverarbeitung

1 Regelungsinhalt / Gegenstand und Dauer der Auftragsdatenverarbeitung / Konkretisierung des Auftragsinhalts (§ 11 Abs. 2 Nr. 2 und Nr. 1 BDSG)

Der Anbieter verarbeitet für den Kunden die in **Anhang 1** aufgeführten personenbezogenen Daten durch Abschluss des dieser Vereinbarung zugrundeliegenden **Leistungsvertrags**.

Die Auftragsdatenverarbeitung betrifft den Plusnet® Tengo-Service Tengo® Centraflex

Soweit die Parteien weitere Verträge schließen, kraft derer der Anbieter für den Kunden Daten im Auftrag verarbeitet, finden die Regelung dieser Vereinbarung Anwendung.

Der Anbieter verpflichtet sich, die personenbezogenen Daten des Kunden ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum zu verarbeiten und zu nutzen. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

2 Verantwortlichkeit

Der Kunde ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Anbieter sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (verantwortliche Stelle im Sinne des § 3 Abs. (7) BDSG).

Aufgrund dieser Verantwortlichkeit kann der Kunde auch während der Laufzeit und bei Beendigung dieser Vereinbarung die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

3 Technisch-organisatorische Maßnahmen zur Verarbeitung personenbezogener Daten (§ 11 Abs. 2 Nr. 3 BDSG)

Der Anbieter gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Anbieter trifft technische und organisatorische Maßnahmen zur angemessenen Sicherung personenbezogener Daten vor Missbrauch und Verlust, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen.

Die technischen und organisatorischen Maßnahmen sind im **Anhang 2** dieser Vereinbarung beschrieben. Sie unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Anbieter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Der Anbieter wird dem Kunden bei wesentlichen Änderungen schriftlich über diese Änderungen informieren.

Vereinbarung zur Auftragsdatenverarbeitung

4 Berichtigung, Sperrung und Löschung von personenbezogenen Daten (§ 11 Abs. 2 Nr. 4 BDSG)

Der Anbieter hat personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß Leistungsvertrag und Weisung des Kunden zu berichtigen, zu löschen oder zu sperren. Der Kunde hat das Recht, den Anbieter zur Berichtigung, Löschung oder Sperrung anzuweisen. Soweit ein Betroffener sich unmittelbar an den Anbieter zwecks Berichtigung, Sperrung oder Löschung seiner personenbezogenen Daten wenden sollte, wird der Anbieter dieses Ersuchen an den Kunden weiterleiten.

5 Kontrollen und sonstige Pflichten des Anbieters (u.a. § 11 Abs. 2 Nr. 5 BDSG)

Der Anbieter hat zusätzlich im Rahmen der Auftragsdatenverarbeitung nach § 11 Abs. 4 BDSG folgende Pflichten:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Kunden zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Kunden zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG und Ermittlungen im Rahmen der §§ 43, 44 BDSG beim Anbieter.
- Der Anbieter erteilt dem Kunden jederzeit Auskünfte, soweit seine Daten und Unterlagen betroffen sind.
- Der Anbieter stellt auf Anforderung dem Kunden die für eine Übersicht nach § 4g Absatz (2) Satz 1 BDSG notwendigen Angaben zur Verfügung.
- Die Erfüllung der vertraglichen Pflichten ist durch den Anbieter zu kontrollieren und in geeigneter Weise nachzuweisen

6 Pflichten des Kunden

- Der Kunde hat den Anbieter unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.
- Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gemäß § 4g Absatz (2) Satz 2 BDSG liegt beim Kunden.
- Dem Kunden obliegen die aus § 42a BDSG resultierenden Informationspflichten.

7 Unterauftragsverhältnisse (§ 11 Abs. 2 Nr. 6 BDSG)

Dem Kunden sind bei jeder Unterbeauftragung Kontroll- und Überprüfungsrechte über die Einhaltung von Datenschutzvorschriften beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Kunden, vom Anbieter auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

8 Kontrollrechte des Kunden (§ 11 Abs. 2 Nr. 7 BDSG)

Der Kunde hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Einvernehmen mit dem Anbieter durchzuführen. Der Kunde ist berechtigt, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Anbieter in dessen Geschäftsbetrieb zu überzeugen. Der Anbieter verpflichtet sich, den Kunden auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Kunden nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Leistungsvertrages trägt der Anbieter dafür Sorge, dass sich der Kunde von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, können durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO/IEC 27001) erbracht werden.

9 Mitteilung bei Verstößen des Anbieters (§ 11 Abs. 2 Nr.8 BDSG)

Der Anbieter unterrichtet den Kunden unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Kunden.

Der Anbieter hat im Einvernehmen mit dem Kunden angemessene Maßnahmen zur Sicherung der personenbezogenen Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Kunden Pflichten nach § 42a BDSG treffen, wird der Anbieter ihn hierbei im Rahmen seiner Verantwortlichkeiten unterstützen.

10 Weisungsbefugnis des Kunden (§ 11 Abs. 2 Nr. 9 BDSG)

Der Umgang mit personenbezogenen Daten durch den Anbieter erfolgt ausschließlich im Rahmen der vertraglich festgelegten Vereinbarungen. Der Kunde hat ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der personenbezogenen Datenverarbeitung, das durch Einzelweisungen konkretisiert werden kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen den Parteien abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Anbieter nur nach vorheriger schriftlicher Zustimmung durch den Kunden erteilen.

Mündliche Weisungen wird der Kunde unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Anbieter verwendet die für den Kunden verarbeiteten personenbezogenen Daten für keine anderen Zwecke.

Der Anbieter hat den Kunden unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Anbieter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bei dem Kunden bestätigt oder geändert wird. Sollten von einer solchen Verzögerung zwischen den Parteien vereinbarte Service Level bzw. Fristvereinbarungen betroffen sein, so werden diese während der Verzögerung ausgesetzt, sofern und soweit der Anbieter eine Verletzung der Service Level nicht anderweitig zu vertreten hat.

Erteilt der Kunde Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, hat Plusnet ein außerordentliches Kündigungsrecht. Macht Plusnet hiervon keinen Gebrauch, sind die durch die Weisung begründeten Kosten vom Kunden zu tragen.

11 Löschung von personenbezogenen Daten und Rückgabe von Datenträgern (§ 11 Abs. 2 Nr. 10 BDSG)

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Kunden – spätestens mit Beendigung der Leistungsvertrages – hat der Anbieter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden auszuhändigen oder nach vorheriger Zustimmung des Kunden datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, darf der Anbieter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Der Anbieter kann sie dem Kunden zu seiner Entlastung bei Vertragsende übergeben.

Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Kunde.

12 Sonstiges

Sind aufgrund von Gesetzesänderungen oder sonstigen behördlichen Vorgaben neue, hierin nicht vereinbarte Leistungen zu erbringen, so sind diese als kostenpflichtiger Leistungsänderung zu vergüten.

Plusnet
Wir leben Kommunikation

Vereinbarung zur Auftragsdatenverarbeitung

Anhang 1: Auflistung der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten durch den Anbieter sind folgende Datenarten bzw. Datenkategorien.

Datenart bzw. Datenkategorie	**Art der Datenverarbeitung**	**Tengo® Cntraf-lex**
Personenstammdaten	Anlage vom Namen des Nutzers in Verbindung mit der geschäftlichen Telefonnummer, E-Mailadresse und Anschrift im Nutzerverzeichnis des Kunden durch den Kunden oder einen durch den Kunden beauftragten Dritten.	X
Kommunikationsdaten (z.B. E-Mail)	Sämtliche Datenarten, die der Nutzer und sein Kommunikationspartner nach eigenem Ermessen austauschen, und solche, die der Nutzer ablegt.	
Verkehrsdaten im Sinne des TKG (z.B. IP-Adressen, A- und B-RN, Beginn, Ende und Dauer einer Verbindung)	Telefonverbindungsdaten werden im Falle der Beauftragung von Einzelverbindungsnachweisen durch den Kunden in den Systemen der Plusnet für die Dauer von längstens sechs Monaten gespeichert.	X
Kundenhistorie	Im Auftragssystem der Plusnet werden Daten zu den beauftragten Services je Kunde gespeichert.	X
Vertragsabrechnungs- und Zahlungsdaten	Im Abrechnungssystem der Plusnet werden Vertragsdaten sowie Informationen zu Zahlungen und Abrechnungen hinterlegt.	X
Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)	Im Rahmen der Auftragserteilung werden Auskunftsdaten von Dritten zur Bonitätsprüfung herangezogen.	X

Vereinbarung zur Auftragsdatenverarbeitung

Anhang 2: Technische und Organisatorische Maßnahmen

Dieser Anhang beschreibt die technischen und organisatorischen Maßnahmen des Anbieters zum Zeitpunkt des Vertragsschlusses. Der Kunde wird über Änderungen informiert, soweit sie von nicht nur unwesentlicher Bedeutung für die beauftragte Leistung ist.

a. Organisationskontrolle

Organisation	Anforderung	Status
Organisatorische Maßnahmen zur Sicherstellung der Verarbeitung personenbezogener / sensibler Daten	IT-Sicherheitskonzeption	Eine Informationssicherheitsmanagement-Leitlinie ist in der aktuellen Version für die Standorte Hamburg, Nürnberg und München vorhanden und kann vor Ort eingesehen werden.
	IT-Sicherheitsrichtlinie	Eine Informationssicherheitsmanagement-Richtlinie ist in der aktuellen Version vorhanden und kann vor Ort eingesehen werden.
	Kennwortrichtlinie	Die Kennwortrichtlinie ist in der aktuellen Version vorhanden und kann vor Ort eingesehen werden.
	Datenschutzrichtlinie	Eine Datenschutzrichtlinie für die Standorte Hamburg, Nürnberg und München ist aktuell vorhanden und kann vor Ort eingesehen werden.
	Zertifizierungen	Der Anbieter ist zum Zeitpunkt der Vertragsunterschrift zertifiziert nach: ISO 9001:2008 ISO 27001:2005 für die in den Zertifikaten aufgeführten Standorte (Stand Juli 2013: Hamburg, Nürnberg, München). Der Anbieter ist zum Zeitpunkt der Vertragsunterschrift am Unternehmensteil Hamburg geprüft nach: IDW PS 951 A und B
	Risikomanagement	Ein Konzern-Risikomanagement ist etabliert und berichtet regelmäßig an den Vorstand.
	Notfallplanung	Eine Notfallplanung ist etabliert und getestet.
	Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist hauptamtlich gestellt und dem Vorstandsvorsitzenden direkt unterstellt.

Vereinbarung zur Auftragsdatenverarbeitung

Organisation	Anforderung	Status
	Verpflichtung der Mitarbeiter nach § 5 BDSG und § 88 TKG	Die Mitarbeiter des Anbieters werden bei Einstellung auf die Einhaltung des Datengeheimnisses, des Datenschutzes, und des Fernmeldegeheimnisses verpflichtet und soweit notwendig auf das Sozialgeheimnis. Eine Sensibilisierung erfolgt bei Einstellung bzw. regelmäßig.

b. Zutrittskontrolle

Zutritt	Anforderung	Status
Schutz der Räume mit Datenverarbeitungsanlagen vor dem Zutritt Unbefugter	Eingezäuntes Betriebsgelände	Die Betriebsgelände der Rechenzentren sind umzäunt.
	Alarmanlage, Video- / Fernsehmonitor: zu beachten: § 6b BDSG	Sensible Gebäude bzw. Gebäudeteile werden mit einer Videoanlage, z.T. mit Bewegungsmeldern und einer Einbruchmeldeanlage überwacht. Die Videoüberwachung berücksichtigt § 6b BDSG und ist mit Hinweisschildern kenntlich gemacht.
	Personenkontrolle beim Gebäudezutritt	Alle Mitarbeiter des Anbieters haben zu jeder Zeit Zugang zu den allgemein zugänglichen Räumlichkeiten des Unternehmens. Zutritte zu anderen Sicherheitszonen werden nur auf Anforderung und nach Freigabe durch einen Freigabeberechtigten freigeschaltet. Die Überprüfung der Zutrittsberechtigungen erfolgt in regelmäßigen Abständen durch die Fachabteilungen. Als Besucher gelten alle Personen, die nicht Mitarbeiter des Anbieters sind. Alle Besucher haben sich beim Empfang anzumelden und sind in die Besucherliste ein- und auszutragen sowie im Haus zu begleiten. Alle externen Handwerker, Haus- und RZ-Techniker müssen sich zu Beginn ihrer Arbeiten am Empfang anmelden. Dieser informiert den Mitarbeiter, der den Besuch erwartet und veranlasst die Abholung. Ist weder der gewünschte Mitarbeiter noch ein anderer Mitarbeiter, der mit der Aufgabe für den externen Handwerker, Haus- oder RZ-

Vereinbarung zur Auftragsdatenverarbeitung

Zutritt	Anforderung	Status
		Techniker vertraut ist, erreichbar, darf kein Zutritt gewährt werden.
	Zutrittskontrollsystem, Ausweisleser, Magnetkarte, elektr. Türöffner	Die Zutrittssteuerung an den Standorten, an denen Daten erhoben und verarbeitet werden können (Köln, Hamburg, Nürnberg und München) erfolgt über ein Zutrittskontrollsystem (Magnetkarten mit elektronischem Türöffner). Das System regelt und kontrolliert den Zutritt zum Grundstück und zu den Gebäuden. Das Zutrittskontrollsystem integriert alle vorhandenen Ausweistechnologien mit analogen und digitalen Sensoren sowie einem Alarmmanagement.
		Mit Hilfe des Zutrittskontrollsystems wird festlegt, wer wann das Grundstück oder Gebäude betreten darf und wann den einzelnen Personen zu welchen Bereichen Zutritt gewährt wird.
	Schlüssel / Schlüsselvergabe	Die Schlüsselvergabe erfolgt bei Bedarf durch den Wachdienst oder das zentrale Gebäudemanagement. Jeder ausgegebene Schlüssel wird in einem Schlüsselbuch oder in einem Schlüsselmanagementsystem
	Weitere Überwachungseinrichtungen	An sensiblen Standorten: 7 x 24 Stunden Wachdienst, regelmäßige Kontrollgänge; Videoüberwachung und Bewegungsmelder in den RZ-Fluren

Vereinbarung zur Auftragsdatenverarbeitung

c. Zugangskontrolle

Zutritt	Anforderung	Status
Schutz der Computersysteme gegen den Zugang für Unbefugte	Zugang zu Systemen nur über Zugangsberechtigungen	Der Zugang zu den Systemen erfolgt grundsätzlich über eine Nutzerkennung und ein entsprechend sicheres Kennwort.
	Berechtigungen nur nach Genehmigung durch Vorgesetzte	Die Zugangsberechtigung wird über einen elektronischen Workflow beantragt und von der verantwortlichen Stelle genehmigt.
	Besondere Berechtigungen nur nach Genehmigung durch Beauftragte	Besondere Berechtigungen (z. B. Systemadministrator) werden über einen elektronischen Workflow beantragt und genehmigt.
	Einrichtung eines Nutzerstammsatzes pro User	Für jeden Nutzer wird gemäß Auftrag ein Nutzerstamm angelegt.
	Kennwortverfahren (Mindestlänge, regelmäßiger Wechsel)	Das Kennwortverfahren ist in der Kennwortrichtlinie dokumentiert (s. a. Abschnitt a). Bezüglich Passwortlänge, Komplexität, Gültigkeit und Historie existieren verbindliche Vorgaben.
	Protokollierung und Kontrolle fehlerhafter Anmeldungen	Fehlerhafte Anmeldungen werden protokolliert und bei Bedarf ausgewertet.
	Automatische Sperrung PC (z. B. Kennwort oder Pausenschaltung)	Eine automatische Sperrung des PC erfolgt nach 10 Minuten.

d. Zugriffskontrolle

Zutritt	Anforderung	Status
Schutz der Daten gegen den Zugriff durch Unbefugte	Zugriff auf Daten nur über Zugriffsberechtigungen	Der Zugriff auf Daten erfolgt über eine Nutzerkennung und ein entsprechend sicheres Kennwort sowie den entsprechend zugewiesenen Zugriffsberechtigungen (Rollen).
	Berechtigungen nur nach Genehmigung durch Vorgesetzte	Die Zugriffsberechtigungen (Rollen) werden über einen elektronischen Workflow beantragt und genehmigt.
	Besondere Berechtigungen nur nach Genehmigung durch Beauftragte der Plusnet	Besondere Zugriffsberechtigungen (Rollen) werden über einen elektronischen Workflow beantragt und genehmigt.
	Regelungen zum Entzug von Zugriffsberechtigungen	Der Entzug von Zugriffsberechtigungen (Rollen) erfolgt über einen elektronischen Workflow.

Vereinbarung zur Auftragsdatenverarbeitung

Zutritt	Anforderung	Status
	Berechtigungsvergabe nur durch autorisierte Personen	Berechtigungsvergaben erfolgen nur anhand eines elektronischen Workflows durch autorisierte Personen.
	Kontrolle der Berechtigungsvergaben	Eine Kontrolle der Berechtigungsvergaben erfolgt regelmäßig.
	Verpflichtungserklärungen für Administratoren	Die Mitarbeiter des Anbieters werden bei Einstellung auf die Einhaltung des Datengeheimnisses, des Datenschutzes, und des Fernmeldegeheimnisses verpflichtet und soweit notwendig auf das Sozialgeheimnis. Eine Sensibilisierung erfolgt bei Einstellung bzw. regelmäßig.
	Schulungen der Administratoren	Administratoren werden regelmäßig im Umgang mit Informationssicherheit speziell geschult.
	Kontrollierte Vernichtung von Daten und Ausdrucken	Die kontrollierte Vernichtung von Daten und Ausdrucken erfolgt durch spezialisierte, zertifizierte Dienstleister.

e. Weitergabekontrolle

Weitergabe	Anforderung	Status
Schutz der Daten bei der Speicherung oder Übermittlung gegen unbefugtes Kopieren, Verändern oder Löschen	Geschützte Räume zur Datenaufbewahrung	Die Lagerung der Datensicherungen erfolgt entweder in einem geschützten Raum (z. B. Datenschutzraum, Rechenzentrum) des Anbieters oder extern durch einen entsprechenden Dienstleister.
	Schutzmaßnahmen für Datenübertragung übers Internet	Die Datenübertragung über das Internet erfolgt geschützt (z.B. verschlüsselt, per TLS).

Vereinbarung zur Auftragsdatenverarbeitung

f. Eingabekontrolle

Eingabe	Anforderung	Status
Nachweis der Dateneingabe oder -veränderung	Änderungen am System	Eingeführter Change-Prozess zur Freigabe und Dokumentation von Zeitpunkt, Dauer und Auswirkung sowie Zuständigkeit für die durchgeführte Änderung.
	Einsatz von Systemen mit Protokollfunktionen	Soweit möglich werden Systeme mit Protokollfunktion eingesetzt.
	Aufbewahrung von Systemprotokollen	Systemprotokolle werden im Rahmen der gesetzlichen/vertraglichen Vorgaben aufbewahrt.

g. Auftragskontrolle

Auftrag	Anforderung	Status
Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen den Parteien	Kriterien zur Auswahl des Auftragnehmers und des Vertriebspartners	Evaluationsverfahren durch den Einkauf des Anbieters, Auswahl von Vertriebspartner durch Fachabteilung
	Prüfungen bei potentiellen Auftragnehmern	Evaluationsverfahren durch den Einkauf des Anbieters, Auswahl von Vertriebspartner durch Fachabteilung.
	Bewertung der IT-Sicherheit vor Auftragsentscheidung	Eine Bewertung der IT-Sicherheit des Auftragnehmers erfolgt vor Auftragsvergabe durch den Einkauf und durch die fachlich verantwortliche Stelle; Zertifizierungsverfahren bei Vertriebspartnern
	Eindeutige Vertragsgestaltung	Eine eindeutige Vertragsgestaltung mit Abgrenzung der Rechte und Pflichten der Parteien untereinander, zu Auftragnehmern und Vertriebspartnern wird mit formalisierten Verträgen und Auftragsformularen sichergestellt.
	Kontrolle der Vertragsausführung	regelmäßige Überprüfung, Vorlage von Prüfungsberichten
	Weisungen	Auf Ziffer 10 des Auftragsdatenverarbeitungsvertrags (oben) wird verwiesen.

h. Verfügbarkeitskontrolle

Verfügbarkeit	Anforderung	Status
Schutz der Daten gegen zufällige Zerstörung oder Verlust	Regelmäßige Datensicherungen	Eine Datensicherung erfolgt regelmäßig.
	Unterbrechungsfreie Stromversorgung (USV)	Die Rechenzentren des Anbieters sind durch getrennte USV Anlagen mit Batteriepufferung und Dieselgeneratoren gegen Stromausfälle gesichert. Redundante Hauseinführungen sind implementiert für die Rechenzentren in Hamburg, Nürnberg und München
	Getrennte Aufbewahrung	Die Datensicherung erfolgt auf räumlich getrennte Systeme.
	Virenschutz / Firewall	Der Anbieter betreibt auf allen Systemen zentral gemanagte Virenscanner sowie vorgeschaltete Firewallsysteme.
	Notfallplan	Der Anbieter verfügt über einen Notfallplan und entsprechende Handbücher zur Aufrechterhaltung der Kernprozesse im K-Fall.

i. Trennungskontrolle

Trennung	Anforderung	Status
Trennung der Datenbestände, die zu unterschiedlichen Zwecken verarbeitet werden	"Interne Mandantenfähigkeit" der Systeme	Die durch den Anbieter eingesetzten Systeme sind mandantenfähig.
	Zweckbindung der Systeme	Die Systeme werden gemäß den im Leistungsvertrag skizzierten Anforderungen zweckgebunden verwendet.
	Zweckbindung der Daten	Die Daten werden gemäß den im Leistungsvertrag skizzierten Anforderungen zweckgebunden verarbeitet.

j. Remote Zugriff auf Systeme des Anbieters

Remote Zugriff	Anforderung	Status
„Remote Zugriff“ auf Systeme des Anbieters	Sichere Anbindung für „Remote Zugriff“ durch Mitarbeiter und Subunternehmer des Anbieters	Der „Remote Zugriff“ aus dem „Home Office“ auf Systeme des Anbieters ist mit Anbieter-eigenen PCs und Laptops möglich. Zusätzlich besteht die Möglichkeit der Einwahl auf einen Terminalserver, wobei

Vereinbarung zur Auftragsdatenverarbeitung

Remote Zugriff	**Anforderung**	**Status**
		hierzu ein Passwort und ein RSA Token benötigt wird (2-Faktor Authentifizierung). In beiden Fällen erfolgt der Remote Zugriff über einen gesicherten VPN-Tunnel. Die Daten werden verschlüsselt übertragen.
	Zugang zu Systemen nur über Zugangsberechtigungen	Der Zugang zu den Systemen erfolgt über eine Nutzerkennung und ein entsprechend sicheres Kennwort.
	Berechtigungen nur nach Genehmigung durch Vorgesetzte	Die Zugangsberechtigung wird über einen elektronischen Workflow beantragt und genehmigt.
	Besondere Berechtigungen nur nach Genehmigung durch Beauftragte	Besondere Berechtigungen (Systemadministrator) werden über einen elektronischen Workflow beantragt und genehmigt.
	Kennwortverfahren (Mindestlänge, regelmäßiger Wechsel)	Das Kennwortverfahren ist in der Kennwortrichtlinie dokumentiert (s. a. Abschnitt a). Bezüglich Passwortlänge, Komplexität, Gültigkeit und Historie existieren verbindliche Vorgaben.
	Protokollierung und Kontrolle fehlerhafter Anmeldungen	Eine Protokollierung und Kontrolle fehlerhafter Anmeldungen erfolgt.
	Automatische Sperrung PC (z.B. Kennwort oder Pausenschaltung)	Eine automatische Sperrung des PCs erfolgt nach 10 Minuten.
	Regelungen zum Entzug von Zugriffsberechtigungen	Der Entzug von Zugriffsberechtigungen (Rollen) erfolgt über einen elektronischen Workflow.