ALLNET Computersysteme GmbH

ASP/SaaS-Vereinbarung zur Auftragsverarbeitung

Stand 09.07.2021 Version 1.1

Diese Vereinbarung zur Auftragsdatenverarbeitung gilt für die Nutzung sämtlicher Produkte der Allnet Computersysteme GmbH, Maistraße 2, 82110 Germering (im Folgenden: „**ALLNET**“ als Auftragsverarbeiter), die wir unseren Kunden (im Folgenden: „**Kunde**“ als Verantwortlicher und Auftraggeber) im Wege des Application Service Providing („ASP“) oder als Software as a Service („SaaS“) zur Verfügung stellen und bei denen wir personenbezogene Daten verarbeiten.

Präambel

Diese Vereinbarung ergänzt und konkretisiert die Verpflichtungen der Parteien aus den mit uns geschlossenen Verträgen zur Nutzung von ASP/SAaaS-Leistungen, bei denen Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten i. S. v. Art. 4 Nr. 1 DS-GVO des Kunden in Berührung kommen können, in Bezug auf den Datenschutz.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1. Der Gegenstand, Art und Zweck der Auftragsverarbeitung ist in den Einzelverträgen und der jeweiligen Leistungsbeschreibungen beschrieben.
1.2. Die Verarbeitung umfasst je nach Vertragstyp die nachfolgend genannten Arten von Daten: Personenstammdaten, Kommunikationsdaten, Zeitstempel, Medieninhalte, Messdaten, Konfigurationsdaten und sonstige personenbezogene Daten.
1.3. Folgende Kategorien von Personen sind von der Verarbeitung betroffen: bei Verträgen mit Verbrauchern: der Vertragspartner als Inhaber des Nutzerkontos; bei Verträgen mit Unternehmern: Geschäftsführer, leitende Angestellte, Beschäftigte; bei Enterprise- und White-Label-Lizenzen: zusätzlich Kunden bzw. Abonnenten des Kunden, sonstige betroffene Personen.
1.4. Die Laufzeit dieser Vereinbarung richtet sich nach dem Buchungszeitraum der Einzelverträge, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet im Europäischen Wirtschaftsraum statt. Der Kunde stimmt zu, dass ALLNET eine Verlagerung in ein Drittland durchführen kann, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Anwendungsbereich und Verantwortlichkeit

2.1. ALLNET verarbeitet personenbezogene Daten im Auftrag des Kunden. Dies umfasst Tätigkeiten, die in den Einzelverträgen und in den Leistungsbeschreibungen konkretisiert sind. Der Kunde bleibt hinsichtlich der Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

2.2. ALLNET verarbeitet die Daten ausschließlich im Rahmen der Weisungen des Kunden. Die Weisung besteht aus den in den Einzelverträgen und der Leistungsbeschreibung anfänglich festgelegten Weisungen. Änderungen von Weisungen können vom Kunden im Rahmen der jeweiligen Funktionalität unmittelbar im Rahmen der Verwaltung eines Benutzerkontos erteilt werden, andernfalls in schriftlicher Form oder in Textform an ALLNET.

2.3. ALLNET wird den Kunden unverzüglich informieren, wenn ALLNET der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. ALLNET ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

3. Pflichten des Auftragsverarbeiters

3.1. ALLNET darf personenbezogene Daten von betroffenen Personen nur im Rahmen der Weisungen des Kunden verarbeiten. Sofern ALLNET durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, informiert ALLNET den Kunden vor Beginn der Verarbeitung über diesen Umstand, sofern das betreffende Recht eine solche Information nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2. ALLNET wird im eigenen Verantwortungsbereich die innerbetriebliche Organisation datenschutzkonform gestalten, insbesondere durch die in Anhang 1 beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der personenbezogenen Daten „TOMs“.

Die Maßnahmen der Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten. Dem Kunden sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten.

3.3. ALLNET behält sich eine Änderung der technischen und organisatorischen Maßnahmen nach billigem Ermessen vor, gewährleistet jedoch, dass das gesetzliche und vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.4. ALLNET unterstützt den Kunden im Rahmen der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Hierfür kann ALLNET eine angemessene Vergütung verlangen.

3.5. ALLNET gewährleistet, dass es die mit der Verarbeitung der personenbezogenen Daten des Kunden befassten Mitarbeiter und anderen für ALLNET tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisungen des Kunden zu verarbeiten. Ferner gewährleistet ALLNET, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- oder Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.6. ALLNET unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt werden. ALLNET trifft die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

3.7. ALLNET ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten nach Art. 37 DS-GVO zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Dessen Kontaktdaten werden dem Kunden zum Zweck der direkten Kontaktaufnahme zur Verfügung gestellt. Kontaktinformationen des ersten Ansprechpartners in Datenschutzfragen und des Datenschutzbeauftragten sind unter der Datenschutzerklärung verfügbar.

3.8. ALLNET gewährleistet, den Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

3.9. Die Berichtigung und Löschung von personenbezogenen Daten obliegt dem Kunden. Gleiches gilt für die Einschränkung der Verarbeitung von personenbezogenen Daten.

3.10. Die personenbezogenen Daten werden nach dem Ende des Buchungszeitraums gelöscht. Es obliegt dem Kunden, Sicherungskopien von seinen personenbezogenen Daten anzufertigen und die personenbezogenen Daten vor Vertragsende umzuziehen. Für ALLNET besteht, sofern in den Einzelverträgen nicht anders vereinbart, keine Pflicht zur Herausgabe von personenbezogenen Daten, auf die der Auftraggeber selbst Zugriff hat.

3.11. ALLNET verpflichtet sich zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO.

4. Pflichten des Kunden

4.1. Dem Kunden obliegt es, ALLNET personenbezogene Daten rechtzeitig zur Leistungserbringung zur Verfügung zu stellen. Der Kunde ist für die Qualität der personenbezogenen Daten allein verantwortlich. Er hat ALLNET unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Verarbeitungsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

4.2. Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichten sich der Kunde und ALLNET, sich bei der Abwehr des Anspruches gegenseitig zu unterstützen. Kontaktinformationen des ersten Ansprechpartners in Datenschutzfragen und des Datenschutzbeauftragten sind in der Datenschutzerklärung verfügbar.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder Auskunft über die personenbezogenen Daten an ALLNET, wird ALLNET dieses Ersuchen unverzüglich an den Kunden weiterleiten, sofern eine Zuordnung an den Kunden nach den Angaben der betroffenen Person möglich ist.

6. Nachweismöglichkeiten

6.1. ALLNET weist dem Kunden auf Anfrage die Einhaltung der in Art. 28 DSGVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

6.2. Sollten im Einzelfall weitere Kontrollen durch den Kunden oder einen von diesem beauftragten Prüfer erforderlich sein, so sind Anfragen in schriftlicher Form zu stellen. ALLNET darf diese von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung durch den Kunden oder den von diesem beauftragen Prüfer abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu ALLNET stehen, hat ALLNET gegen diesen ein Widerspruchsrecht. Der Widerspruch ist in Textform gegenüber dem Kunden zu erklären.

6.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Kunden eine Kontrolle vornehmen, gilt grundsätzlich 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6.4. Für die Unterstützung bei der Durchführung einer Kontrolle nach 6.2 oder 6.3 kann ALLNET eine angemessene Vergütung verlangen, sofern nicht Anlass der Kontrolle der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich von ALLNET ist. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Kontrolle vom Kunden glaubhaft zu machen.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1. Der Kunde stimmt zu, dass ALLNET Subunternehmer hinzuzieht. Sofern bereits anfänglich Subunternehmer zum Einsatz kommen, übergibt ALLNET dem Kunden vor Beginn der Datenverarbeitung eine entsprechende Liste mit deren vollständigen Anschriften. Vor der Hinzuziehung weiterer oder der Ersetzung bisheriger Subunternehmer informiert ALLNET den Kunden mit einer Frist von 4 Wochen vorab in Textform. Der Kunde kann der Hinzuziehung oder Ersetzung nur aus wichtigem Grund innerhalb einer Frist von 14 Tagen widersprechen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Hinzuziehung oder Ersetzung als erteilt. Liegt ein wichtiger Grund vor, der von ALLNET nicht durch Anpassung des Auftrages beseitigt werden kann, kann der Kunden diesen Vertrag sowie den mit ihm in Zusammenhang stehenden Einzelvertrag außerordentlich kündigen. Erteilt ALLNET Aufträge an Subunternehmer, wird ALLNET die datenschutzrechtlichen Pflichten aus diesem Vertrag auch auf den Subunternehmer übertragen.

7.2. Auf schriftliche Aufforderung des Kunden hat ALLNET jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmer zu erteilen.

7.3. Die Regelungen in dieser Ziffer 7 gelten auch, wenn ein Subunternehmer in einem Drittstaat in Übereinstimmung mit den Anforderungen der Art. 44 ff DSGVO eingeschaltet wird.

8. Haftung

8.1. Es gelten die Haftungsregelungen der Einzelverträge.

8.2. Der Kunde stellt ALLNET von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen ALLNET aufgrund der vom Kunden beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer weisungswidrigen Verarbeitung der personenbezogenen Daten durch ALLNET beruht.

9. Informationspflichten, Schriftformklausel, Rechtswahl

9.1. Sollten die personenbezogenen Daten des Kunden bei ALLNET durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat ALLNET den Kunden unverzüglich darüber zu informieren. ALLNET wird alle Dritten in diesem Zusammenhang unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Kunden als Verantwortlicher im Sinne der DSGVO liegt.

9.2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung, die auch in Textform erfolgen kann. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.3. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Einzelvertrages vor.

ALLNET Computersysteme GmbH

ANLAGE ZUM VERTRAG ÜBER DATENVERARBEITUNG IM AUFTRAG (AVV) - TECHNISCH ORGANISATORISCHE MASSNAHMEN „TOMs“

Stand 09.07.2021 Version 1.1

Folgende technische und organisatorische Maßnahmen sind von ALLNET als Auftragsverarbeiter umgesetzt und mit dem Kunden vereinbart.

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung von personenbezogenen Daten

1.1. Pseudonymisierung

Pseudonymisierung ist die Verarbeitung von personenbezogenen Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Unsere Maßnahmen in Zusammenhang mit der Pseudonymisierung personenbezogener Daten bestehen in:

☐ Auswahl eines geeigneten Pseudonymisierungsverfahrens nach dem aktuellem Stand der Technik

☐ Pseudonymisierungsgebot ist zentraler Bestandteil im Rahmen des Datenschutzkonzepts des Unternehmens

☐ Pseudonymisierung von Daten nach einem risikobasierten Ansatz entsprechend unterschiedlicher Schutzbedarfskategorien von Daten

☐ Einsatz von Software, die ein sicheres Management pseudonymisierter Daten erlaubt

☐ Gesicherte Aufbewahrung der zur Pseudonymisierung verwendeten kryptographischen Schlüssel bzw. Kontrolllisten (ggf. verschlüsselte Speicherung der Kontrolllisten)

☐ Berechtigungskonzept für Zugriff auf kryptographischen Schlüssel bzw. Kontrolllisten, die eine Personalisierung ermöglichen

1.2. Verschlüsselung

Unter Verschlüsselung ist ein Verfahren zu verstehen, durch das eine klar lesbare Information in eine nicht lesbare bzw. interpretierbare Zeichenfolge umgewandelt wird.

Unsere Maßnahmen im Zusammenhang mit der Verschlüsselung von Daten bestehen in :

☐ Verschlüsselung von vertraulichen Daten beim Transport und über Datennetze

☐ Verschlüsselung von vertraulichen Daten bei der Speicherung auf IV-Endgeräten und mobilen Datenträgern

☐ Verschlüsselung von streng vertraulichen Daten bei der Speicherung auf Datenträgern (Festplatten)

☐ Durchführung einer Risikoanalyse, wenn kryptografische Maßnahmen nicht durchführbar sind

☐ Anweisungen zum Einsatz abgestimmter und freigegebener kryptographischen Verfahren

☐ Algorithmen, Anwendungen und Standards

☐ Erzeugung von Schlüsselmaterial für produktive Systeme bei einer Public Key Zertifizierungsstelle

☐ Geheimhaltung der privaten Schlüssel eines Zertifikats

☐ Schutz vor unberechtigtem Zugriff oder Ausspähung von geheimen Schlüsseln sowie der privaten Schlüssel der Public Key Kryptographie

☐ Löschung bzw. Vernichtung von nicht mehr benötigten Schlüsseln auf eine sichere Art

2. Maßnahmen zur Gewährleistung der Vertraulichkeit

Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem auch solche, die zur Zutritts-, Zugriffs- oder Zugangskontrolle gehören. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, vor versehentlichem Verlust, versehentlicher Zerstörung oder Beschädigung.

2.1. Zutrittskontrolle

2.1.1. Zutritt zu Geschäftsräumen von ALLNET

☐ Maßnahmen, die umgesetzt sind, Unbefugten den Zutritt zu Geschäftsräumen von ALLNET, in denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☐ Weitere Sicherheitsmaßnahmen (wie z.B. Videoüberwachung, Türzustandsüberwachung von Ein-, Ausgängen und Fluchttüren, Sicherung der Peripherie durch Zäune, Werkschutz) können in Abhängigkeit der Risikoeinstufung des jeweiligen Standorts umgesetzt sein

☐ Festlegung zutrittsberechtigter Personen

☐ Zutrittskontrolleinrichtungen unter Einsatz personalisierter und codierter Ausweiskarten, persönlich ausgehändigter Schlüssel

☐ Zutrittsregelung für betriebsfremde Personen

☐ Einrichtung verschiedener Sicherheitszonen mit verschiedenen Zutrittsberechtigungen

☐ Dokumentation der Vergabe und des Entzugs von Zutrittsberechtigungen

☐ Videoüberwachung

☐ Einbruchsmeldeanlage mit Alarmübertragung zur ununterbrochenen besetzten Sicherheitsleitstelle bzw. zur Polizei

☐ Türzustandsüberwachung für Eingänge/Ausgänge

☐ Fluchttürüberwachung

☐ Restriktive Schlüsselregelungen

☐ Besucheraufenthalte nur in Begleitung von Beschäftigten von ALLNET

☐ Ausweistragepflicht

2.1.2. Zutritt zu Serverräumen von ALLNET

Maßnahmen, die zusätzlich zu den oben genannten Sicherheitsmaßnahmen unternommen werden, um Unbefugten den Zutritt zu den Serverräumen von ALLNET, in denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren sind nachfolgend aufgeführt. In Abhängigkeit der Risikoeinstufung des jeweiligen ALLNET-Serverraums können weitere Sicherheitsmaßnahmen (wie z.B. Videoüberwachung) umgesetzt sein.

☐ Protokollierung des Zutritts zu Serverräumen (automatisch durch Zutrittskontrollsystem oder durch ausgelegte Listen)

☐ Videoüberwachung im Serverraum

☐ Türzustandsüberwachung für Serverräume

☐ Automatische Türzuzieheinrichtung bei Ein- und Ausgängen in Serverräumen

☐ Aufenthalte von Fremdfirmen/Techniker in Serverräumen nur unter ständiger Aufsicht von Beschäftigten von ALLNET

2.1.3. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten benutzt werden können

Vorgaben zur Festlegung von Passwörtern:

☐ Mindestlänge

☐ Verwendung von Merkmalen (Zeichen, Sonderzeichen, Zahlen)

☐ Verwendung von Trivialpasswörtern

☐ Änderungsintervalle

☐ Verbot der Weitergabe von Kennwörtern

☐ Speicherung und Übermittlung in Datenverarbeitungssystemen

Vorgaben der zu verwendenden Anwendungen zur Verwaltung von Kennwörtern

☐ Sperrung des Bildschirmes bei Inaktivität nach Zeit

☐ Sperren von Benutzernamen bzw. zeitliche Verzögerungen der Anmeldeversuche nach mehrfachen fehlerhaften Zugangsversuchen

☐ Regelmäßige Zugangsberechtigungsprüfungen für den Benutzerzugang zum Netzwerk von:

☐ Beschäftigen

☐ Externen

Regelmäßige Zugangsberechtigungsprüfungen für Administratoren von:

☐ Netzwerken und Netzwerkdiensten

☐ Servern

☐ Risikobehafteten Anwendungen

☐ Abschottung interner Netzwerke durch Einrichtung von Firewall-Systemen

☐ Verwendung von Virtual Private Networks (VPN) mit User/Kennwort als Authentisierungsmerkmal

☐ Maschinenzertifikat als Authentisierungsmerkmal

☐ Restriktive Vorgaben zur Sperrung von USB-Ports

☐ Nutzung einer zentralen Verwaltungssoftware für Smartphones (z.B. für löschen von Daten auf

dem Smartphone)

2.1.4. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Informationen zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☐ Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen

☐ Berechtigungskonzept auf Anwendungsebene mit differenzierten Berechtigungsstufen (z.B. Rollen)

☐ Protokollierung der vergebenen Zugriffsberechtigungen

☐ Einsatz von Signaturen und Zertifikaten zur Sicherstellung von Urheberschaft

☐ Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend Schutzklassenkonzept

2.2. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

☐ Logische bzw. technische Trennung von Daten

☐ Benutzerprofile / Trennung von Nutzerkonten

☐ Unterschiedliche Zugriffsberechtigungen

☐ Speicherung in spezifischen Speicherbereichen

☐ Trennung der verarbeitenden Systeme

3. Maßnahmen zur Gewährleistung der Integrität

Maßnahmen zur Umsetzung des Gebots der Integrität sind zum einen solche, die auch zur Eingabekontrolle gehören, zum anderen aber solche, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen.

3.1. Weitergabekontrolle

Maßnahmen, die 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.

☐ Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit insbesondere mittels Datei- und Festplattenverschlüsselung auf Hard- oder Softwarebasis.

☐ Verschlüsselung der Übertragung von Daten in Abhängigkeit von deren Schutzbedürftigkeit insbesondere bei der Übertragung über öffentliche Netze.

☐ Verwendung von Virtual Private Networks (VPN)

☐ Beim physischen Transport: Benutzung sicherer verschließbarer Transportbehälter beim

☐ Transport von Backup-Datenträgern

☐ Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend

☐ Schutzklassenkonzept

☐ Sorgfältige Auswahl von Transportpersonal

3.2. Eingabekontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

☐ Gesetzeskonforme Vertragsgestaltung von Verträgen über die Datenverarbeitung personenbezogener Daten mit Subunternehmern mit entsprechender Regelung von Kontrollmechanismen

☐ Einholung von Selbstauskünften bei Dienstleistern bezüglich deren Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen

☐ Schriftliche Bestätigung von mündlichen Weisungen

☐ Aufzeichnung und bedarfsgerechtes Vorhalten von geeigneten Aktionen (z.B. Logfiles)

☐ Einsatz von Protokollierungs- und Protokollauswertungssystemen

☐ Festlegung der Befugten für die Erstellung von Datenträgern und der Bearbeitung von Daten

4. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit

4.1. Verfügbarkeitskontrolle

Damit sind Maßnahmen gemeint, die gewährleisen, dass personenbezogene Daten gegen zufälligen Untergang oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.

☐ Zentrale Beschaffung von Hard- und Software

☐ Einsatz zentral geprüfter und freigegebener Standardsoftware aus sicheren Quellen

☐ Regelmäßige Durchführung von Datensicherungen bzw. Einsatz von Spiegelungsverfahren

☐ Außerbetriebnahme von Hardware (insbesondere von Servern) erfolgt nach einer Überprüfung der darin eingesetzten Datenträger und ggf. nach erfolgter Sicherung der relevanten Datensätzen

☐ Unterbrechungsfreie Stromversorgung (USV) im Serverraum

☐ Getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden.

☐ Mehrschichtige Virenschutz- und Firewall-Architektur

☐ Notfallplanung (Notfallplan für Sicherheits- und Datenschutzverletzungen mit konkreten Handlungsanweisungen)

☐ Feuer-/Wasser- und Temperaturfrühwarnsystem in den Serverräumen

☐ Brandschutztüren

☐ Betreuung der IT durch qualifizierte und ständig weitergebildete Mitarbeiter

☐ Regelmäßiges Testen der Datenwiederherstellung entsprechend dem Sicherheitskonzept

4.2. Auftragskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten, die im Auftrag bei einem Subunternehmer von ALLNET verarbeitet werden, nur entsprechend den Weisungen und Anforderungen an die Datenverarbeitung des Kunden verarbeitet werden können.

Kriterien zur Auswahl der Auftragnehmer festlegen (Referenzen, Zertifizierungen, Gütesiegel)

☐ Detaillierte schriftliche Regelungen (Vertrag/Vereinbarungen) der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes, auch zum Einsatz von Subunternehmern, eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten

☐ Sicherstellung, dass die Auftragsdurchführung kontrolliert und dokumentiert wird

☐ Vertragliche Vereinbarung mit Subunternehmern, eigene und externe Mitarbeiter auf das Datengeheimnis zu verpflichten

4.3. Belastbarkeitskontrolle

Hierzu gehören Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Provider zu ergreifen sind. Darüber hinaus ist auch eine kontinuierliche Überwachung der Systeme erforderlich.

☐ Load-Balancing

☐ Dynamische Prozesse und Speicherzuschaltung

☐ Penetrationstests

☐ Regelmäßige Belastungstests der Datenverarbeitungssysteme

☐ Belastungsgrenze für das jeweilige Datenverarbeitungssystem im Voraus über das notwendige Minimum ansetzen

☐ Regelmäßige Schulung des eingesetzten Personals entsprechend dem Gebot zur Sicherstellung der Integrität und Vertraulichkeit der Datenverarbeitung zu handeln

5. Maßnahmen zur Wiederherstellung der Verfügbarkeit

Zur Sicherstellung der Widerherstellbarkeit sind einerseits ausreichende Sicherungen erforderlich, wie aber auch Maßnahmenpläne, die im Sinne von Katastrophen-Fall-Szenarien den laufenden Betrieb wiederherstellen können.

☐ Regelmäßige Back-Up der Datenbestände und Einsatz von Spiegelungsverfahren

☐ Redundante Datenspeicherung

☐ Doppelte IT-Infrastruktur für Verarbeitungen mit hohen Verfügbarkeitsanforderungen

☐ Backup Rechenzentrum im Fall von Sabotage oder kritischen Umweltereignissen

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung erfolgt im Rahmen der Durchführung von:

☐ internen Prüfungen durch die zuständigen Stellen (z.B. Revision, Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Prozesskontrollen durch Qualitätsmanagement)

☐ externen Prüfungen durch Auditoren, Zertifizierungsstellen