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

0☐ 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