Anlage 3

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO der roda computer GmbH:

1.Präambel

Der Gesetzgeber hat in Art. 32 Abs.1 der DS-GVO (Datenschutz Grundverordnung) angeordnet, dass die Maßnahmen zur Sicherung der Datenverarbeitungsvorgänge der Auftragsdatenverarbeitung einzuhalten sind. Der Auftraggeber hat bei Missachtung mit empfindlichen Bußgeldern bis hin zum Verbot der Datenverarbeitung zu rechnen. Die roda computer GmbH (nachfolgend: Auftragnehmer) unterstützt den Auftraggeber bei der Einhaltung dieser gesetzlichen Anforderungen, indem sie es dem Auftraggeber mit dieser Allgemeinen Bedingung zum Datenschutz ermöglicht, die gesetzlichen Anforderungen des Art. 32 Abs1 DS-GVO umsetzen.

2.Vertraulichkeit (Art. 32 Abs. 1 lt. B DS-GVO)

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Das Gelände und das Gebäude sind rund um die Uhr kameraüberwacht. Die Videos werden gemäß Aufbewahrungsfrist des Sicherheitskonzeptes gespeichert. Es gibt Bewegungsmelder die außen das Licht einschalten und innen einen Alarm auslösen. Außerhalb der Betriebsstunden ist ein Wachschutz für Gebäude durch externe Dienstleister engagiert. Fenster und Türen sind alarmgesichert. Die Alarmanlage hat eine Aufschaltung zur Polizei. Das Gebäude mit administrativen Räumen ist umzäunt und wird außerhalb der Betriebsstunden verschlossen. Der Zutritt zu dem Unternehmen erfolgt für die Besucher (inklusive Techniker und Kunden) ausschließlich über die Zentrale. Die Türen zur Lieferantenanfahrt des Rechenzentrums werden von hier zum Zutritt berechtigter und angemeldeter Personen freigeschaltet. Laut Dienstanweisung bewegen sich Besucher und Dienstleister nie alleine im Gebäude und tragen dauerhaft einen Besucherausweis bzw. ein Dienstleisterausweis. Jeder Besucher muss sich am Empfang anmelden. Der Zutritt betriebsfremder Personen wird an dieser Stelle protokolliert. Alle Techniker und Kunden müssen Ihren Besuch 24 Stunden im Voraus anmelden, damit die Legitimation des Besuches überprüft werden kann. Der unbeaufsichtigte Zugang zum Gebäude (nur für Mitarbeiter) erfolgt über RFID Token in Kombination mit einem Passwort / PIN im Rechenzentrumsgebäude und über ein elektronisches Türsystem mit PIN im Hauptgebäude.

Zutritt zu dem Rechenzentrum

Die Serversysteme werden im Rechenzentrum der WortmannAG, der TERRA CLOUD GmbH im Bereich des Housing, betrieben. Der Zugang zum Treppenhaus (zu dem Bereich Housing) ist vergittert. Bewegungsmelder und Kameras sichern diesen Bereich zusätzlich ab.

Der Zugang zu den Serverfluren des Bereich Housing erfolgt über Token/PIN, die zentral gemanagt werden. Die Vergabe der RFID Token unterliegt einem dokumentierten Berechtigungsprozess. (Mitarbeiter der Terra Cloud haben einen Master-Key für Notfälle, welcher verschlossen abgelegt ist). Alle Türen innerhalb des Rechenzentrums geben Alarm, wenn sie länger als der erlaubte Zeitraum (wenige Sekunden) offenstehen. Dieser Zustand wird auf der Videowand überwacht.

Der Serverraum des Auftragnehmers hat keine Verbindung zur Außenhaut des Gebäudes. Der Zugang zu dem Serverraum des Auftragnehmers wird automatisch protokolliert. Alle Zugangsprotokolle werden gemäß

Aufbewahrungsfrist des Sicherheitskonzeptes gespeichert. Es finden täglich Kontrollgänge statt (hierbei wird auf mögliche Probleme und Veränderung geachtet).

Zutritt Housing

Zutritt erfolgt über RFID & PIN sowie zusätzlich Schlüssel zu dem Käfig. Die Zutritte werden protokolliert. Die einzelnen Serverschränke sind von einem Käfig umgeben. Der Schlüssel zu dem Käfig liegt bei dem administrativen Team der WORTMANN AG.

Zutritt Räume für (Hardware) Support

Zutritt erfolgt über elektronisches Türschlosssystem mittels PIN. Die Zutritte werden protokolliert.

Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Alle internen Systeme der roda computer GmbH sind an ein Active Directory angeschlossen. Die Zugänge sind besonders gesichert und haben besondere Anforderungen an die Passwörter:

- Mind. 8 Zeichen
- Bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen
- Wechsel alle 90 Tage
- Die Passwörter dürfen nicht aus Namen, Wörtern oder Tastaturmustern bestehen

Bei Inaktivität des Benutzers ist laut Vorgabe die Bildschirmsperre zu aktivieren. Alle Systeme sind über redundante Internet Leitungen (die aus 2 Bundesländern zugeführt werden) mit der Außenwelt verbunden. Diese Verbindungen werden durch mehrere zentrale Firewall Systeme abgesichert. Die Regelwerke dieser Firewall werden in kurzen Abständen überarbeitet. Die Firewalls werden extern von einem professionellen Anbieter gepflegt und sowohl intern als auch extern überwacht. Hierdurch wird eine frühzeitige automatische Angriffserkennung gewährleistet. Die verschiedenen Netzwerkbereiche sind über VLAN voneinander getrennt. Darüber hinaus ist eine vorgelagerte Firewall vorhanden, welche bei Verbindungen von/nach extern greift.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Es liegt ein anwenderbezogenes Berechtigungskonzept vor, dass im Active Directory umgesetzt wird. Die realisierte Berechtigungsstruktur bezieht sich auf das gesamte System des Unternehmens: Die Berechtigungen können auf Dateien, auf Datensätze, auf Anwendungsprogramme und das Betriebssystem differenziert werden und die Lese-, Änderungs- und Löschrechte einschränken. Es wird sichergestellt, dass jeder Benutzer nur auf die Daten zugreifen kann, zu denen er zugriffsberechtigt ist. Das Berechtigungskonzept, dass sich an den Stellungen der Mitarbeiter orientiert, ist schriftlich festgehalten (Dokumentation über das Active Directory). Weiterhin ist das Berechtigungskonzept programmtechnisch in der Anwendung, im Active Directory hinterlegt. Sämtliche Zugriffe der Benutzer werden protokolliert.

Bei den Systemen wird sehr differenziert auf die Notwendigkeit des Zugriffs durch die Mitarbeiter geachtet. Jeder Zugriff eines Mitarbeiters wird protokolliert. Der Schutz vor externen unberechtigten Zugriffen erfolgt durch Einsatz von Mehr-Stufiger Firewall-Architektur und Netzwerksegmentierung.

Trennungskontrolle

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

Das Trennungsgebot wird zur räumlichen Trennung von Housing (Server) und dem Backup-System (extra Leitung) umgesetzt, wobei diese jeweils einen eigenen Brandabschnitt darstellen. Für besonders kritische Systeme werden die Backupdaten zusätzlich in einem 2. Standort vorgehalten.
Im Housing werden die Schränke und Server innerhalb eines Käfigs installiert. Das Backup-System verfügt über eine eigene Versorgung und ist durch eine 256 Bit AES Verschlüsselung gesichert. Das verwendete Passwort ist nur den Administratoren der WORTMANN AG bekannt und kann durch externe Personen nicht zurückgesetzt oder ausgelesen werden.
Es werden Systeme und Programme eingesetzt, welche eine notwendige Mandantentrennung ermöglichen bzw. das Datenbankprinzip der Trennung über Zugriffsregelungen umsetzen. Test- und Produktionsumgebungen bzw. Test- und Produktionsdaten sind voneinander getrennt.

Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

3.Integrität (Art. 32 Abs. 1 lit. B DS-GVO)

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.

Die öffentlichen IP Adressen werden von speziell geschulten Mitarbeitern gepflegt und vergeben. Auch die VLANs werden nur von speziell geschulten Mitarbeitern gepflegt. Die Pflege der Systeme wird durch ein Administrations-Team der WORTMANN AG/roda computer GmbH gewährleistet.

Es gibt für unterschiedliche Systembereiche eigene Netze. Diese sind voneinander durch VLANs getrennt. Das indirekte Patchen erfolgt über WSUS. Darüber hinaus werden Serversysteme mit verschiedene Applikationen durch ein zentrales Managementsystem mit Updates versorgt. Weiterhin ist ein zentraler Virenscanner im Einsatz bzw. werden Systeme über eine zentrale Scansoftware geprüft.

Beim Office System ist ein Virenschutz auf allen Rechnern, zentral in der Firewall, auf dem Mailserver und auf den internen Servern umgesetzt. Der gesamte Virenscanner und die gesamte Konfiguration werden zentral gepflegt.

Die Entsorgung von defekten oder nicht mehr benötigten Datenträgern erfolgt durch ein zertifiziertes Entsorgungsunternehmen. Im Rahmen von Wartungs- oder Garantieansprüchen werden Datenträger der Kunden temporär in einem gesicherten Bereich gelagert bis diese je nach Auftrag gehandhabt werden.

Die Nutzung von privaten Datenträgern ist technisch unterbunden durch Deaktivierung der Schnittstellen (USB) an Client-Systemen. Ausnahmen laufen durch einen protokollierten Genehmigungsprozess und diese Client-Systeme unterliegen zusätzlichen technischen Überprüfungen (zentrale Scansoftware) sowie Protokollierung.

Bei Verwendung von Transportunternehmen bzw. generell Transport, werden Datenträger bzw. Systeme mit Datenträger derart verpackt, dass eine Beschädigung dieser möglichst ausgeschlossen werden kann. Ein Nachweisverfahren über den Versand (zum Beispiel Begleitzettel, Versandschein) sowie den Eingang beim Empfänger (zum Beispiel Empfangsbestätigung) kommt zum Einsatz.

Es werden regelmäßig Backups von allen kritischen Systemen erstellt. Dabei werden physikalische Backups als verschlüsselter Stream erstellt und in einem anderen Brandabschnitt elektronisch zugänglich aufbewahrt. Die Verschlüsselung der Backup Datensätze ist obligatorisch und erfolgt kundenseitig. Die Passwörter für die Verschlüsselung sind nur der WORTMANN AG bekannt und können nicht von externen Personen, z.B. Hersteller der Backupsoftware, ausgelesen oder zurückgesetzt werden.

Eingabekontrolle

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

Alle Zugriffe auf die Management Systeme werden protokolliert. Große und/oder kritische Konfigurationsänderungen werden über einen Projektmanagementprozess durchgeführt, protokolliert und archiviert.

Zur Gewährleistung der Eingabekontrolle sind die vom Softwarehersteller mitgebrachten Log Mechanismen und Transaktionsprotokolle, zur Protokollierung aller Eingaben für alle Anwendungen, vorhanden. Im Rahmen des Auftrags- bzw. Supportmanagement ist die im System mitgebrachte Historienlog bzw. Protokollierung der Tätigkeiten vorhanden.

4.Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DS-GVO)

Verfügbarkeitskontrolle

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

Es werden Backups nach einem Backup-Plan durchgeführt. Die Backups aller kritischen Systeme liegen in getrennten Brandabschnitten. Für einige kritische Datenbanken liegen diese zusätzlich in einem 2. Standort.

Die Stromversorgung der Server erfolgt über eine Ringeinspeisung. Diese ist dem Unternehmen vertraglich zugesichert.

Das Unternehmen setzt eine redundante unterbrechungsfreie Stromversorgung (USV) ein, in der Blitz- und Überspannungsschutzeinrichtungen integriert sind. Die unterbrechungsfreie Stromversorgung wird

automatisch einmal pro Quartal hinsichtlich ihrer Wirksamkeit getestet. Die USV kann das gesamte Rechenzentrum 20 Minuten mit Strom versorgen. Für die weitere Stromversorgung bei Stromausfall steht ein Notstromaggregat, versorgt über einen Dieseltank mit einem Volumen von fünf Tagen, zur Verfügung. Das Notstromaggregat wird hinsichtlich der Wirksamkeit einmal im Monat getestet.

Die Verbindung zum Internet wird über zwei verschiedene, physikalisch getrennte Leitungen aus zwei verschiedenen Bundesländern realisiert. Die beiden Leitungen sind nicht gekreuzt.

Die Kühlung der Serverräume wird bis zu 90 % des Jahres über eine Luftkühlung umgesetzt. Hierzu werden zwei Klimaanlagen redundant betrieben. Beide Anlagen sind verschaltet, somit stehen beide passiven Kühlflächen der Chiller zur Verfügung. Zum Schutz gegen Wasser sind Feuchtigkeits- und Leckage Sensoren im gesamten Gebäude verbaut. Auch verfügt das Unternehmen über Wasser-Auffangwannen an allen notwendigen Stellen und über Entwässerungs-Anlagen und Drainagen auf dem Grundstück. Weiterhin besteht in den Serverbereichen ein 60 cm hoher Doppelboden.

Bei der Löschanlage handelt es sich um eine N2 Löschanlage mit Brandmeldeanlage und Brandfrüherkennung. Die Brandmeldeanlage verfügt über eine direkte Aufschaltung zur Feuerwehr. Auch gibt es spezielle Feuerlöscher vor Ort. Für den weiteren Brandschutz werden regelmäßige Begehungen durch die Feuerwehr durchgeführt. Auch führt die Feuerwehr regelmäßige Schulungen zu Löscheinsätzen im Rechenzentrum durch.

Es wird ein zentrales Patch-Management mit physikalisch getrennter Testumgebung eingesetzt. Die kritischen Serversysteme laufen in einem RAID-Verbund. Kritische Systeme für die Auftragsdatenverarbeitung liegen redundant vor.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutzmanagement

Maßnahmen durch innerbetriebliche Organisation, die die Einhaltung der Anforderungen und Verpflichtungen des Datenschutzes sicherstellen.

Mitarbeiter bestätigen bei Eintritt in das Unternehmen Anweisungen u.a. über datenschutzrechtliche Verpflichtungen über eine Vertraulichkeitsvereinbarung. Es werden jährlich wiederkehrende Schulungen zu innerbetrieblichen Organisation und Einhaltung von Anweisungen mit anschließenden Test durchgeführt. Der Nachweis der Schulung ist über eine Protokollierung der Durchführung durch den Mitarbeiter vorhanden.

Der Datenschutzbeauftrage für die Wortmann AG ist schriftlich bestellt und die Fachkundenachweise des Datenschutzbeauftragen liegt vor. Die Datenschutzbeauftragte der Wortmann AG ist auf https://www.wortmann.de/impressum hinterlegt.

Incident-Response Management

Im Rahmen des Notfallmanagement ist dieser Prozess definiert. Im Zuge der jährlichen Schulung wird dieser an alle Mitarbeiter kommuniziert bzw. aktualisiert.

Datenschutzfreundliche Voreinstellung (Art. 25 Abs. DS-GVO)

Systeme sind derartig konfiguriert, dass nur die notwendigen Daten zur Datenverarbeitung aufgenommen/abgefragt werden.

Auftragskontrolle

Maßnahmen, die prüfen, dass sich der Dienstleister bei der Verarbeitung von personenbezogener Daten an die Weisungen des Auftraggebers hält.

Es liegt ein formalisiertes Auftragsmanagement vor mit schriftlichen Verträgen und Vereinbarungen. Bei (Hardware)Supportleistungen werden nach Prüfung der Zulässigkeit der Auftragsdatenverarbeitung die handschriftlichen Notizen bzw. telefonischen Anweisungen der Kunden als Basis für die Vertragstätigkeiten genommen.

Es erfolgt eine sorgfältige Auswahl der Dienstleister unter anderem nach dem Niveau seiner technisch-organisatorischen Maßnahmen. Ggf. werden Sicherheitsmaßnahmen festgelegt, welcher der Dienstleister umzusetzen hat. Alle Dienstleister werden einmal im Jahr durch den Auftragsnehmer kontrolliert.