Anhang TOM

Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO

1 Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

1.1 Pseudonymisierung

Maßnahmen zur Verarbeitung personenbezogener 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

Personenbezogene Daten werden, soweit vom Auftraggeber angewiesen, für Verarbeitungen pseudonymisiert.

Es besteht eine Festlegung der Rollen, welche zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind.

Eine Pseudonymisierung kann durch eine Verschlüsselung oder durch das Entfernen sämtlicher personenbezogener Daten für bestimmte Verarbeitungen erfolgen. Die Vorgaben werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und konkretisiert.

1.2 Verschlüsselung

Einsatz von Verfahren und Algorithmen, die personenbezogene Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Es kommen symmetrische und asymmetrische Verschlüsselungstechniken in Betracht

Im Sinne der Auftragsverarbeitung entscheidet allein der Auftraggeber, wann welche Verschlüsselung für seine Verarbeitung eingesetzt werden kann, dieses können z.B. sein: Data at Transport – Data at Rest – Ende-zu-Ende.

Ein Fernzugriff (Remote) erfolgt über eine VPN (Virtual Private Network) Anbindung oder verschlüsselt zum Terminal Server.

Mobile Datenträger enthalten keine personenbezogenen Daten und sind für Betriebs- und Geschäftsunterlagen immer verschlüsselt.

Die Verschlüsselungen entsprechen dem Stand der Technik.

Ein Zugriff oder die Nutzung von Inhalten erfolgt nur im Rahmen der beauftragten Verarbeitung und auf Weisung des Auftraggebers.

2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren

Die Gelände, auf denen sich die Rechenzentren des Dienstleisters befinden, unterliegen strengen Sicherheitsvorgaben.

Für diese Gebäudeteile existieren Sicherheitsmaßnahmen wie ein patrouillierender Werkschutz, Einbruchmeldeanlagen, Kameraüberwachungen der Innen- und Außenzugänge der Rechenzentren rund um die Uhr.

Innerhalb der Gebäude sind verschiedene Sicherheitszonen definiert, z.B. Leitstandzone, Serverflächen, Segmente des Auftraggebers, Datenarchiv.

Ein Zutrittsberechtigungskonzept regelt die Zutrittsberechtigung nur autorisierter Personen durch verschiedene und unabhängige Zutrittssysteme. Ferner gewährleisten Zutrittskontrollen einen ausschließlich autorisierten Zutritt für Mitarbeiter des Unternehmens. Der Zutritt zu einzelnen Produktionsbereichen und dem Geschäftsbereich wird über sichere Zutrittskontrollsysteme unter Einsatz z.B. von Magnetkarten oder mechanischen Schließmechanismen (z.B. Türschlösser) beschränkt. Die Schlüsselausgabe wird in einem Schlüsselbuch dokumentiert.

Der Zugang zu den einzelnen Produktionsbereichen ist für Besucher oder externe Dienstleister nur in Begleitung von autorisiertem Personal gestattet.

2.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

Alle Systeme und Anwendungen erfordern eine Authentifizierung zur Nutzung der Dienste.

Der Zugriff auf die verarbeitenden Systeme erfolgt mit einer eindeutigen persönlichen User-ID und einem Passwort.

Folgende Anforderungen an die Passwortgüte werden mindestens eingehalten: Eine Mindestlänge von 8 Zeichen, bestehend aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen, automatische Sperrung nach mehrfacher Falscheingabe, Passworterneuerung nach Ablauf der maximalen Gültigkeitsdauer, Trivialkennwortprüfung.

Für die Mitarbeiter wird ein Starter-Changer-Leaver Prozess durchlaufen. Hier wird durch die verantwortlichen Führungskräfte zur Durchführung einer Benutzerkontrolle die Autorisierung basierend auf dem „least privilege principle“ vorgenommen.

Systemadministration und reguläre Benutzer erhalten getrennte Benutzerkonten. Ebenfalls findet für privilegierte

Rechte ein regelmäßiger Check bzgl. vorhandener Autorisierung statt.

Zur Vermeidung des Risikos ist bei Remote Zugriff die Nutzung von 2-Faktor-Authentifizierungsmethoden umgesetzt.

Zum Schutz sämtlicher Netzwerke gegen Zugriffe von außen werden Zugriffe durch Firewalls reguliert und erfolgt standardmäßig über eine Sicherheitsinfrastruktur-Kette aus Proxy, Virenscanner und Firewall.

Es bestehen darüber hinaus feste Regelungen für den Zugriff auf EDV Systeme.

Die An- und Abmeldungen der Benutzer an den DV-Anlagen werden protokolliert.

Beim Verlassen des Arbeitsplatzes ist dieser zu sperren oder herunterzufahren, es ist eine Voreinstellung zur automatischen Sperrung nach spätestens 10 Minuten implementiert.

Zudem existiert ein Zugangsberechtigungskonzept. Generell sind alle Berechtigungen entzogen und müssen freigeschaltet werden. Das Zugangsberechtigungskonzept basiert auf dem Prinzip von Benutzerrollen und -profilen. Die Vergabe der personalisierten Berechtigungen erfolgt nur durch die dafür zuständige Abteilung.

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Regelungen zur Verfügung gestellt werden.

2.3 Zugriffskontrolle

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

Es besteht ein Berechtigungskonzept für den Zugriff auf die DV-Systeme.

Zugriffsrechte werden entsprechend dokumentiert, vergeben, entzogen bzw. gelöscht, sobald sich die Tätigkeit des Mitarbeiters ändert.

Die Zugriffrechte werden nach dem Minimalprinzip / “Need-To-Know“-Prinzip vergeben. Es werden nur so viele Zugriffsrechte vergeben, wie es für die Aufgabenwahrnehmung notwendig ist. Die Einhaltung des „Need-To-Know“-Prinzips liegt in der Verantwortung der autorisierten Führungskraft.

Die Zugriffskontrolle basiert auf einem rollenbasierten Berechtigungskonzept für Systemzugriffe und abgestufte Administrationsrechte entsprechend der Aufgabengebiete. Alle administrativen Tätigkeiten werden grundsätzlich auf den Systemen protokolliert und können somit nachvollzogen und nachgewiesen werden.

Bei der Einrichtung eines Zuganges erhält der Benutzer nur minimale Standardberechtigungen. Diese dürfen nur über festgelegte Beantragungswege erweitert werden, wobei die jeweiligen Vorgesetzten bzw. Verantwortlichen zur Einhaltung einer angemessenen Funktionstrennung im Berechtigungsprozess ihre Zustimmung geben müssen (4-Augen-Prinzip).

Ein Fernzugriff (Remote Access) erfolgt über eine VPN (Virtual Private Network) Anbindung oder verschlüsselt zum Terminal Server.

Es sind nur autorisierte Speichermedien zu verwenden und eine Speicherung von personenbezogenen Daten des Auftraggebers auf mobilen Datenträgern ist nur auf Weisung des Auftraggebers gestattet.

Auf Anfrage können entsprechende Konzepte und Prozessdokumentationen zur Verfügung gestellt werden.

2.4 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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

Um das Risiko für den Betroffenen zu vermindern sind die Mitarbeiter anzuweisen, nur sichere Datenübertragungswege zu nutzen. Die mögliche Datenübertragung kann über vertrauenswürdige Leitungen und Netze, welche ein Mitprotokollieren nicht ohne Weiteres ermöglichen, erfolgen.

Datenübertragungen erfolgen innerhalb des gesicherten Netzwerkes (z.B. mit entsprechender Verschlüsselung). Die elektronische Übertragung von Daten auf öffentlichen Wegen bzw. über öffentliche Netze findet ausschließlich auf verschlüsselten Wegen statt.

Unterschiedliche Optionen, wie beispielsweise die Nutzung von SSL-Zertifikaten für eine verschlüsselte Web-Kommunikation, SSL-Virtual Private Netzwerk für eine gesicherte Verbindung (abgesicherter Remote Access), Elektronische Signatur, Protokollierung, werden auf Anfrage des Auftraggebers umgesetzt.

Im Sinne der Auftragsverarbeitung entscheidet allein der Auftraggeber, welche Daten übermittelt werden, welcher Übertragungsweg und welche Übertragungsart umgesetzt werden. Hier können Netzsegmente zusätzlich durch Access Control-Listen voneinander abgeschottet und das gesamte Netzwerk durch mehrstufige Firewall-Systeme abgesichert werden. Muss bei der Übertragung eine nicht vertrauenswürdige Datenleitung verwendet werden, so kann die Übertragung auch verschlüsselt (z.B. über Virtual Private Network - VPN, Transport Layer Security - TLS, etc.) erfolgen.

Eine Übertragungskontrolle kann durch ein beauftragtes Logging zur Überprüfung, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden, gewährleistet werden.

Die Sicherungen (Backups) von Daten werden in einem Sicherheitsbereich gelagert.

Zur Gewährleistung einer Transportkontrolle erfolgt ein Transport oder Versand von Datenträgern nur, wenn dieser vom Auftraggeber angewiesen wurde. Dieser bestimmt ebenfalls den Transportweg. Dieses unterliegt einem Kontroll- und Dokumentationsprozess.

Eine notwendige Vernichtung von Datenträgern und vertraulicher Dokumente erfolgt durch ein spezialisiertes und zertifiziertes Unternehmen nach der DIN 66399. Bis zur Vernichtung lagern die Datenträger in einem Sicherheitsbereich und sind vor unbefugtem Zugriff geschützt. Die Vernichtung von Datenträgern des Verantwortlichen und die Protokollierung dieser Vernichtung erfolgt nur gemäß Beauftragung und Weisung.

Für die Nutzung von mobilen Datenträgern (USB-Stick, CD, DVD, etc.) existieren Verhaltensregeln. Diese stellen sicher, dass keine personenbezogenen Daten oder Betriebs- und Geschäftsunterlagen auf mobilen Datenträgern abgelegt werden dürfen.

Auf Anfrage können entsprechende Konzepte und Prozessdokumentationen zur Verfügung gestellt werden.

2.5 Trennungskontrolle

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

Eine Trennung der Daten erfolgt auf Weisung des Auftraggebers für seine Daten.

Als Beispiele für eine logische oder physische Trennung auf Mandanten- und/oder Datenebene können benannt werden: die Funktionstrennung von Produktions- / Integrations- / Testsystemen, Einsatz verschiedener Datenbanken, Einsatz von Zugriffskontrollsoftware und Einrichtung von Zugriffsrechten (mit deren Protokollierung), unterschiedliche Verschlüsselung für einzelne Datensätze, logische Trennung (z.B. auf gemeinsam genutzten Systemen), physische Trennung (z.B. auf dedizierten Systemen), etc.

Über ein Berechtigungskonzept werden Zugriffe von Nutzern, die nicht den Zugriffsberechtigungen entsprechen, wirkungsvoll unterbunden.

Auf Anfrage können entsprechende Konzepte und Prozessdokumentationen zur Verfügung gestellt werden.

3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

Eine Eingabekontrolle sowie die Aufbewahrungsfrist der hierdurch entstandenen Daten erfolgt auf Weisung durch den Auftraggeber für seine Daten und auf seiner Infrastruktur oder in seinen Applikationen.

Optionale Protokollierungen sowie revisionssichere Ablage der Logs sind auf Weisung umsetzbar und müssen definiert werden. Administrative Zugriffe auf Systeme können generell durch ein Standard-Logging auf Betriebssystemebene nachvollzogen werden.

Sofern die Eingabe, Veränderung sowie Löschung der Daten auf IT Systemen erfolgen, werden mittels entsprechender Protokollierungs- und Protokollauswertungssysteme die Veränderungen an diesen Daten protokolliert (z.B. Zugriffs-ID, Zugriffszeit, Autorisierung und entsprechende Aktivität).

Eine Auswertung der Eingabekontrolle erfolgt nur bei Bedarf im Rahmen der Weisung durch eine manuelle oder automatisierte Protokollauswertung.

Auf Anfrage können entsprechende Konzepte und Prozessdokumentationen zur Verfügung gestellt werden.

3.2 Organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen /Revision etc.

Weiterführende Ausführungen zur Absicherung von Berechtigungen sind im Kapitel Zugangs- und Zugriffskontrolle ausführlich dokumentiert. Protokollauswertungen sind im Rahmen der Weisung zu beantragen und werden in diesem Umfang durchgeführt.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle

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

Sämtliche Einrichtungen des beauftragten Rechenzentrums sind physisch gegen Sicherheitsbedrohungen und Umweltgefahren geschützt.

Folgende Möglichkeiten können auf Anforderung umgesetzt werden: redundante Stromzuführung, hochverfügbare

Stromversorgung (abgesichert durch USV) mit statischen Übergabeschaltern (STS), Dieselaggregate für die Notstromversorgung, Klimatisierung mit hoher Verfügbarkeit, Brandmeldeanlagen mit Brandfrüherkennung und direkter Alarmmeldung bei der örtlichen Feuerwehr, je Rechenzentrum einen eigenen Brandabschnitt, Einbruchmeldeanlage mit Türschließkontrolle, Notfallkonzepte und Havarieplan, redundante Netzanbindungen und Netzwerkinfrastruktur, geclusterte Systeme oder redundante Hardware (von Bauelementen bis zu ganzen Servern – Geo-Redundanz).

Alle Sicherheitseinrichtungen werden regelmäßig auf ihre Betriebs- und Ausfallsicherheit überprüft.

Für ein vollumfängliches Backup, je nach Zweckbindung der jeweiligen Verarbeitung, stehen unterschiedliche Archivierungsmöglichkeiten zur Verfügung, diese können sein: eine regelmäßige automatisch initiierte und überwachte Datensicherung (z. B. einmal pro Kalenderwoche eine Vollsicherung sowie tägliche inkrementelle Sicherungen). Die normale Haltezeit dieser Sicherungen wird auf Weisung umgesetzt. Die Datensicherung kann in einem separaten Backup-System, welches in einem anderen Brandschutzabschnitt oder an einem anderen Standort wie das Produktivsystem steht, erfolgen.

Sämtliche Mitarbeiter unterliegen der Anweisung, keine tätigkeitsrelevanten Daten auf Arbeitsplatzrechnern zu speichern, sondern hierfür eingerichtete Backup-gesicherte Fileserverbereiche zu nutzen.

Auf allen Arbeitsplatzrechnern kommt ein Virenschutz zum Einsatz. Das Vorhandensein eines Virenschutzes sowie die regelmäßige Aktualisierung des Virenpatterns und das zeitnahe Einspielen von Sicherheitsupdates für die genutzten Betriebssysteme und Anwendungsprogramme wird sichergestellt.

Themen rund um das BCM (Business Continuity Management) sind in einem Incident-Response-Management Konzept genau zu beschreiben.

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Konzepten zu entsprechenden Verfahren zur Verfügung gestellt werden.

4.2 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

Der Dienstleister hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.

Mitarbeiter werden über ihre Rollen und Verantwortlichkeiten z.B. im Wege vorbereitender Schulungen instruiert. Der Auftragnehmer hat einen oder mehrere Verantwortliche für die Kontrolle und das Monitoring der Datensicherheitsvorgaben benannt.

Die Daten werden nur gemäß der Weisung des Auftraggebers verarbeitet. Diese Weisungen haben mindestens in Textform und ausschließlich durch berechtigte Personen des Auftraggebers an berechtigte Personen des Auftragnehmers zu erfolgen.

Alle Mitarbeiter sind auf das Datengeheimnis sowie bei relevanten Verarbeitungen nach Spezialverpflichtungen wie z.B. das Fernmeldegeheimnis und das Sozialgeheimnis verpflichtet. Eine Einsichtnahme ermöglicht die Durchführung von stichprobenartigen Kontrollen.

Besichtigungen der Verarbeitungsstätten, Audits und Dokumentationsprüfungen sind durch den Auftraggeber vorzunehmen und werden vom Auftragnehmer unterstützt.

Es werden Dokumente zu Datenschutz- und Datensicherheit, Verantwortlichkeiten und relevanten Verfahren geführt und überprüft. Diese Dokumente sind für den Auftraggeber im Rahmen eines Audits einsehbar.

Mit externen Dienstleistern werden entsprechende Verträge abgeschlossen, welche das Datenschutzniveau dieser Vereinbarung weiterreichen.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1 Datenschutzmanagement

Für sämtliche Bereiche, in denen die Durchführung von Verarbeitungsvorgängen mit personenbezogenen Daten oder besonderen personenbezogenen Daten gem. Artikel 9 DSGVO oder personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten gem. Artikel 10 DSGVO erfolgt, wurde ein Datenschutzbeauftragter bestellt. Der Datenschutzbeauftrage ist dem Auftraggeber benannt worden und steht als Ansprechpartner zur Verfügung.

Im Falle eines Data Breach ist unverzüglich eine Meldung an die E-Mailadresse Datenschutz@arvato-systems.de, mit den notwendigen, vom Gesetzgeber vorgeschrieben Informationen zu senden.

In regelmäßigen Abständen haben interne Audits zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen zu erfolgen. Es besteht eine Kontrollmöglichkeit im Rahmen eines Audits durch den Auftraggeber.

Die Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch organisatorischen Maßnahmen und der Sicherheit der Verarbeitung erfolgt über den folgenden PDCA-Zyklus mit Plan (Entwicklung eines Sicherheitskonzeptes), Do (Einführung von TOMs), Check (Überwachung der Wirksamkeit / Vollständigkeit) und Act (Kontinuierliche Verbesserung) durch den Auftragnehmer.

Die Übermittlung personenbezogener Daten an ein Drittland erfolgt erst nach schriftlicher Freigabe durch den Auftraggeber und unter Hinzuziehung von Standarddatenschutzklauseln.

Ein Sub-Dienstleister gewährleistet in seinem eigenen Verantwortungsbereich eine vom Schutzniveau vergleichbare Umsetzung des Datenschutzmanagements wie der Auftragnehmer.

5.2 Incident-Response-Management

Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen

Die Sicherstellung des Geschäftsbetriebes während einer Notlage oder Großstörung sowie die schnellstmögliche Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste und Verarbeitungen wird gewährleistet und durch regelmäßige Wiederanlaufübungen erprobt.

Maßnahmen, welche die Belastbarkeit der Systeme und Dienste gewährleisten, sind so ausgelegt, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben. Themen rund um die Speicher-, Zugriffs- und Leitungskapazitäten sowie zu Backup und Redundanz-Konzepten sind in der Verfügbarkeitskontrolle detaillierter aufgenommen.

5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die Anforderungen des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen wird für sämtliche Produkte umgesetzt.