Anhang TOM

Technische und organisatorische Maßnahmen der

Arvato Systems Gruppe

Zuordnung Verarbeitungskategorien

Gütersloh, 03. Mai 2019

Inhaltsverzeichnis

1 Einführung

Verantwortliche für die Datenverarbeitung sind gem. Art. 32 DSGVO verpflichtet, technische und organisatorische Schutzmaßnahmen zu treffen, welche die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten.

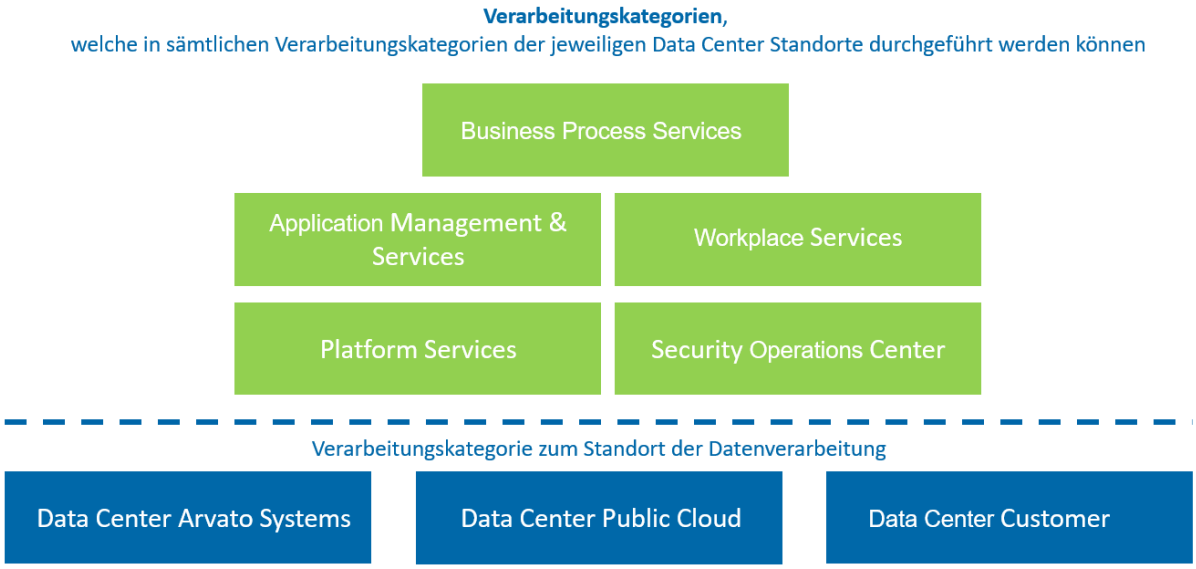
Die Schutzmaßnahmen müssen dabei so gewählt sein, dass durch sie in der Summe ein angemessenes Schutzniveau sichergestellt wird.

Bei Verarbeitungen von personenbezogenen Daten durch Produkte (fertige IPs) ist eine Anpassung und/oder Weisung durch den Auftraggeber nur im Rahmen der Produktmöglichkeiten umzusetzen.

Die Arvato Systems Gruppe* hat sämtliche Verarbeitungen, welche sie für Auftraggeber ausführt, in Verarbeitungskategorien unterteilt. Im nachfolgenden Text sind zu sämtlichen Verarbeitungskategorien kurze Definitionen aufgeführt, welche das Verständnis der Arvato Systems vom Inhalt der jeweiligen Verarbeitungskategorie dokumentieren. Ebenfalls wird dem Auftraggeber je Verarbeitungskategorie, welche im Vertrag zur Auftragsdatenverarbeitung für sein Geschäftsmodell ausgewählt wird, eine Zuordnung zu den jeweils relevanten technischen und organisatorischen Maßnahmen dieser Verarbeitungskategorie ermöglicht.

Diese Übersicht erläutert, welche Schutzmaßnahmen durch Arvato Systems im Hinblick auf die Verarbeitung personenbezogener Daten je Verarbeitungskategorie getroffen sind.

Zur einfacheren Zuordnung des hauptsächlichen Verarbeitungsortes der Daten hat Arvato Systems für den Auftraggeber drei Verarbeitungskategorien mit Data Center Bezug definiert. Dieses ermöglicht eine sofortige Aussage, ob die Hauptverarbeitung in einem der Data Center von Arvato Systems, in einem Data Center eines Public Cloud Dienstleisters (mit dem Arvato Systems den Vertrag mit dem Public Cloud Anbieter geschlossen hat) oder dem Data Center des Auftraggebers (welcher für die Umsetzung seiner technischen und organisatorischen Maßnahmen allein verantwortlich ist) verarbeitet werden.



2 Technische und organisatorische Maßnahmen (TOM) der Arvato Systems Gruppe* für die Verarbeitungskategorien Platform Services, Application Management & Services, Business Process Services, Workplace Services und Security Operations Center

2.1 Definition

Die nachfolgend technischen und organisatorischen Maßnahmen (TOM) gelten nur für die folgenden Verarbeitungskategorien und setzen auf den TOMs des jeweils für die Verarbeitung definierten Data Centers auf:

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

2.2.1 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 möglich und vom Auftraggeber angewiesen, für Verarbeitungen pseudonymisiert:

Durch die Anwendung der Pseudonymisierung auf personenbezogene Daten kann ein Risiko für die betroffene Person gesenkt werden.

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. Hierfür sind die personenbezogenen und personenbeziehbaren Daten für den Empfänger nicht mehr erkennbar und nur noch durch eine identische Kennziffer mit den restlichen Daten zu verbinden, z.B. Trennung von Kundenstammdaten und Kundenumsatzdaten. Die Verarbeitung erfolgt über eine Kennziffer statt über den Namen.

Die Vorgaben werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und in den Leistungsscheinen konkretisiert.

2.2.2 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 eingesetzt werden kann, z.B. 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, welche personenbezogene Daten oder Betriebs- und Geschäftsunterlagen enthalten, müssen immer verschlüsselt werden.

Unterschiedliche Optionen zur symmetrischen oder asymmetrischen Verschlüsselung können auf Anfrage des Verantwortlichen zum Schutz seiner personenbezogenen Daten umgesetzt und in den Leistungsscheinen konkretisiert werden (z.B. Nutzung von SSL-Zertifikaten für eine verschlüsselte Web-Kommunikation, SSL-Virtual Private Netzwerk für eine gesicherte Verbindung).

Die Verschlüsselungen entsprechen dem Stand der Technik.

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

2.3.1 Zutrittskontrolle

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

Für sämtliche Standorte oder Verarbeitungen ohne direkten DC-Bezug gelten die folgende physischen Sicherheitsmaßnahmen.

Zutrittskontrollen gewährleisten einen ausschließlich autorisierten Zutritt für Mitarbeiter des Unternehmens. Der autorisierte Zutritt in Büros erfolgt je nach Standort in der Regelarbeitszeit durch Vereinzelungsschleusen, eine zweite Sicherheitstür, Schließanlagen, Schließzylinder, Türtransponder, autorisierte Mitarbeiterausweise (RFID-Ausweis), automatisierte Zutrittskontrollsysteme (Kartenleser) mit personalisierten Zutrittskarten, Zugangskeys für autorisierte internen Mitarbeiter. Die Schlüsselausgabe wird in einem Schlüsselbuch dokumentiert.

Besucher werden am Eingang durch einen Ansprechpartner abgeholt und während des gesamten Aufenthaltes in den Räumlichkeiten begleitet.

Teilweise patrouilliert der Werkschutz in unregelmäßigen Abständen auf dem Gelände oder die Gebäudeteile sind mit Einbruchmeldeanlagen geschützt. Ebenfalls erfasst an einigen Standorten eine Kameraüberwachung für Innen- und Außenanlagen rund um die Uhr den Eingangsbereich, die Lobby, die Liftanlagen als auch die Zugänge zu den Bürobereichen.

2.3.2 Zugangskontrolle

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

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

Der Zugriff auf die verarbeitenden Systeme erfolgt mit einer eindeutigen persönlichen User-ID und einem Passwort. Die Passwortvergabe erfolgt in Konformität zur Passwortrichtlinie, hier sind z.B. zu benennen: Anforderungen an die Passwortgüte, erzwungene Passwortänderungen oder nach Mehrfachanmelden mit falschem Passwort eine Sperrung des Benutzerkontos zur Vermeidung des Risikos (um Brute-Force-Attacken zu verhindern).

Für privilegierte Rechte findet ein regelmäßiger Check der vorhandenen Autorisierungen statt. Systemadministratoren und reguläre Benutzer erhalten getrennte Benutzerkonten.

Zur Vermeidung des Risikos ist bei Remote Zugriff auf das Netzwerk die Nutzung von 2-Faktor-Authentifizierungsmethoden (Secure-ID Karten oder Zertifikate) in der Informationssicherheitsrichtlinie vorgeschrieben.

Der Schutz sämtlicher Netzwerke gegen Zugriffe von außen wird durch Firewalls reguliert und erfolgt standardmäßig über eine Sicherheitsinfrastruktur-Kette aus Proxy, Virenscanner und Firewall. An einigen Standorten kann hierfür die spezielle Rolle des Network Security Officer zuständig sein.

2.3.3 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

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 werden. 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.

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

2.3.4 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 über interne Richtlinien angewiesen, nur sichere Datenübertragungswege zu nutzen. Die mögliche Datenübertragung kann über vertrauenswürdige Leitungen und Netze, welche ein Mitprotokollieren nicht ohne Weiteres ermöglichen, erfolgen.

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, können auf Anfrage umgesetzt und in den Leistungsscheinen dokumentiert und bewertet werden.

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.

Für die Sicherung (Backup) von Daten werden bewegliche Datenträger und VTL-Libraries genutzt, welche einer automatischen Inventarisierung unterworfen sind und in einem Sicherheitsbereich lagern.

Zur Gewährleistung einer Transportkontrolle erfolgt ein Transport oder Versand von Datenträgern nur, wenn dieser vom Auftraggeber angewiesen wurde. Dieser bestimmt ebenfalls den Transportweg, welcher beispielsweise der Versand per Einschreiben/Wertpaket oder die Verwendung gesicherter/verschlossener Transportbehältnisse sowie spezieller Kurierdienste (verschlüsselter Versand) umfasst. Dieses unterliegt einem Kontroll- und Dokumentationsprozess.

Eine notwendige Vernichtung von Datenträgern erfolgt durch ein spezialisiertes und zertifiziertes Unternehmen nach aktuellen Normen. 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 in der Informationssicherheitsrichtlinie. Diese stellen sicher, dass personenbezogene Daten oder Betriebs- und Geschäftsunterlagen auf mobilen Datenträgern nur verschlüsselt abgelegt werden dürfen. Dieses verhindert im Rahmen der Datenträgerkontrolle das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern.

Für die sichere Vernichtung bzw. die Entsorgung von Datenträgern und vertraulicher Dokumente existieren Verhaltensregeln.

2.3.5 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. Die unterschiedlichen Optionen werden im Leistungsschein für die unterschiedlichen Verarbeitungen definiert und bewertet.

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

Bei einer Tätigkeit per Remote-Zugriff greift der Mitarbeiter auf die bereits vorgegebene Infrastruktur zu, welche ihm eine Verarbeitung im Rahmen der vorher festgelegten Vorgaben ermöglicht.

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

2.4.1 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 im Rahmen des Leistungsscheines definiert werden.

Administrative Zugriffe auf Systeme können durch ein Standard-Logging auf Betriebssystemebene nachvollzogen werden. Dieses dient zum Nachweis einer unbefugten Veränderung oder Löschung von gespeicherten personenbezogenen Daten im Rahmen der Speicherkontrolle.

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

2.4.2 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.

Eine Konkretisierung ist im jeweiligen Leistungsschein aufzunehmen.

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

2.5.1 Verfügbarkeitskontrolle

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

Eine Verarbeitung der Daten durch Mitarbeiter außerhalb der Data Center erfolgt über Remote / WLAN im relevanten Auftraggeber Data Center und unterliegt somit auch der Verfügbarkeit dieses Data Center.

Sämtliche Mitarbeiter unterliegen der Anweisung, keine tätigkeitsrelevanten Daten auf dem Notebook zu speichern, sondern hierfür eingerichtete Backup-gesicherte Filebereiche zu nutzen, um das Risiko eines Verlustes der Daten auszuschließen.

2.5.2 Auftragskontrolle

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

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 nach Spezialverpflichtungen wie z.B. das Fernmeldegeheimnis, das Sozialgeheimnis und das Postgeheimnis verpflichtet. Eine Einsichtnahme ermöglicht die Durchführung von stichprobenartigen Kontrollen.

Data Center-Besichtigungen oder Audits sind in den relevanten Data Center nach der Verhältnismäßigkeit und rechtzeitiger schriftlicher Anmeldung beim verantwortlichen Fachbereich möglich.

Die Organisation und Durchführung eines Audits unterliegt, zum Schutz der personenbezogenen Daten unterschiedlicher Verantwortlicher, der Auditrichtlinie.

2.6 Allgemeingültige Verfahren bei Arvato Systems zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

2.6.1 Datenschutzmanagement bei der Arvato Systems Group

Für sämtliche rechtliche Einheiten der Arvato Systems, in denen das Kerngeschäft 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 externer Datenschutzbeauftragter bestellt, soweit dieses vom Gesetz vorgegeben ist. Als Ansprechpartner in den einzelnen rechtlichen Einheiten steht ein Team aus ausgebildeten Datenschutzbeauftragten, in der Funktion von Datenschutzkoordinatoren, unter der E-Mailadresse Datenschutz@arvato-systems.de, zur Verfügung.

Arvato Systems definiert die Eckpfeiler des Datenschutzes in der Konzerndatenschutzrichtlinie, sowie konkreter in der Arvato Systems internen Datenschutzrichtlinie.

Durch die IT-Revision und den Datenschutzbeauftragten (falls bestellt) werden in regelmäßigen Abständen Audits zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen durchgeführt. Im Rahmen der Verhältnismäßigkeit besteht nach rechtzeitiger Vorankündigung eine Kontrollmöglichkeit im Rahmen eines Audits durch den Auftraggeber.

Als Nachweis, für eine sicherheitsrelevante Verarbeitung, kann Arvato Systems Zertifikate nachweisen. Sie finden die Zertifikate unter folgendem Link: arvato-systems.de/zertifizierungen

Bei Arvato Systems kann ein ISAE-Report zum Nachweis einer ordnungsgemäßen Verarbeitung und der Beachtung der Informationssicherheit erworben werden.

Das Sicherheitskonzept der Arvato Systems ist in der Konzernrichtlinie zur Information-Security-Policy festgeschrieben.

Zur Erhöhung des Schutzniveaus bei der Verarbeitung von personenbezogenen Daten für den Betroffenen ist die interne Datenschutzrichtlinie der Arvato Systems Gruppe* mit genehmigten Verhaltensregeln für alle Mitarbeiter einzuhalten. Ebenfalls wird das Risiko durch ein wirksames Patch-Management, Pentests, Log-Analysen, Beschäftigung mit Websicherheit (z.B. OWASP) und über ein Security Operations Center gewährleistet. Für die technischen und organisatorischen Maßnahmen wird ein risikobasierter Ansatz präferiert.

Die Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und 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).

2.6.2 Incident-Response-Management bei der Arvato Systems Group

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

Im Rahmen des etablierten BCM (Business Continuity Management) zur Sicherstellung des Geschäftsbetriebes während einer Notlage oder Großstörung sowie zur schnellstmöglichen Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste sind Verfahren dokumentiert. Es werden regelmäßig Wiederanlauf-Übungen durchgeführt.

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 im Abschnitt Verfügbarkeitskontrolle detaillierter aufgenommen.

2.6.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) bei der Arvato Systems Group

Die Umsetzung des Datenschutzes wird bei der Produktentwicklung durch die Berücksichtigung eines internen White Paper „Datenschutz in der Produktentwicklung“, sowie einer internen Checkliste zur Berücksichtigung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen begleitet.

3 Verarbeitungskategorie: Data Center Arvato Systems

Data Center Arvato Systems

3.1 Definition Data Center Arvato Systems

In der Verarbeitungskategorie „Data Center Arvato Systems“ fasst die Arvato Systems-Gruppe* alle Verarbeitungen und Dienstleistungen für ihre Auftraggeber zusammen, die im Zusammenhang mit der Bereitstellung und Wartung von Servern, Storage, Netzwerken, Private Cloud oder andere Data Center-Infrastruktur stehen, die sich in einem der Data Center von Arvato Systems befinden.

Diese Verarbeitungskategorie dient dazu, dem Auftraggeber eine räumliche Einordnung seines Datenflusses zu ermöglichen.

Arvato Systems hat die folgenden technischen und organisatorischen Maßnahmen für sämtliche ihrer Data Center standardisiert.

3.2 Technische und organisatorische Maßnahmen für die eigenen Data Center der Arvato Systems Gruppe

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

3.2.1.1 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 möglich und vom Auftraggeber angewiesen, für Verarbeitungen pseudonymisiert:
Durch die Anwendung der Pseudonymisierung auf personenbezogene Daten kann ein Risiko für die betreffende Person gesenkt werden.

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. Hierfür sind die personenbezogenen und personenbeziehbaren Daten für den Empfänger nicht mehr erkennbar und nur noch durch eine identische Kennziffer mit den restlichen Daten zu verbinden, z.B. Trennung von Kundenstammdaten und Kundenumsatzdaten. Die Verarbeitung erfolgt über eine Kennziffer statt über den Namen.

Die Vorgaben werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und in den Leistungsscheinen konkretisiert.

3.2.1.2 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 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, welche personenbezogene Daten oder Betriebs- und Geschäftsunterlagen enthalten, müssen immer verschlüsselt werden.

Unterschiedliche Optionen zur symmetrischen oder asymmetrischen Verschlüsselung können auf Anfrage des Verantwortlichen zum Schutz seiner personenbezogenen Daten umgesetzt und in den Leistungsscheinen konkretisiert werden (z.B. Nutzung von SSL-Zertifikaten für eine verschlüsselte Web-Kommunikation, SSL-Virtual Private Netzwerk für eine gesicherte Verbindung).

Die Verschlüsselungen entsprechen dem Stand der Technik.

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

3.2.2.1 Zutrittskontrolle

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

Die Räume der Data Center schützen die Infrastruktur der Auftraggeber vor unberechtigtem Zutritt und sichern zudem die Hochverfügbarkeit der Gebäudetechnik für den Data Center-Betrieb ab.

Die Gelände, auf denen sich die Data Center befinden, unterliegen strengen Sicherheitsvorgaben zur Zutrittsberechtigung.

Der Zutritt zu den Data Center ist durch verschiedene, unabhängige Zutrittssysteme nur autorisierten Personen gestattet.

Alle Besucher der Data Center werden mit Datum und Uhrzeit ihres Betretens und Verlassens von den Mitarbeitern erfasst. Der Zutritt zum Gelände wird zudem nur für spezielle autorisierte Zwecke eingeräumt und soweit notwendig, werden Instruktionen im Hinblick auf die Sicherheitsanforderungen des Bereichs und zu Notfallverfahren erteilt. Die Autorisierung für den Zutritt zum Rechenzentrum setzt eine Unterschrift unter die persönliche Einwilligung zur Befolgung der Verhaltensregeln und Richtlinien innerhalb der Data Center-Bereiche voraus.

An einigen Standorten patrouilliert der Werkschutz in unregelmäßigen Abständen über das Gelände, zusätzlich sind alle Gebäudeteile des Data Centers mit Einbruchmeldeanlagen geschützt. Ebenfalls erfassen Kameraüberwachungen die Innen- und Außenzugänge der Data Center rund um die Uhr.

Innerhalb der Gebäude können an unterschiedlichen Standorten verschiedene Sicherheitszonen definiert sein, hier sind zu benennen z. B. Leitstandzone, Serverflächen, Datenarchiv, Segmente des Auftraggebers. Der Zutritt erfolgt generell über eine persönlich zugeordnete und kontrollierbare Zutrittskarte der berechtigten Personen. Die Berechtigung für die einzelnen Zonen wird über einen Autorisierungsprozess gesichert und erfolgt ausschließlich gemäß der Notwendigkeit für das Geschäftsmodell.

Jeder externe Besucher wird von einem internen Mitarbeiter während des gesamten Besuches im DC begleitet. Dienstleistern ist der Aufenthalt in den Räumen des DC nur unter Aufsicht gestattet.

3.2.2.2 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. Die Passwortvergabe erfolgt in Konformität zur Passwortrichtlinie. Hier sind z.B. zu benennen: Anforderungen an die Passwortgüte, erzwungene Passwortänderungen oder nach Mehrfachanmelden mit falschem Passwort eine Sperrung des Benutzerkontos zur Vermeidung des Risikos (um Brute-Force-Attacken zu verhindern).

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 auf das Netzwerk die Nutzung von 2-Faktor-Authentifizierungsmethoden (Secure-ID Karten oder Zertifikate) in der Informationssicherheitsrichtlinie vorgeschrieben.

Der Schutz sämtlicher Netzwerke gegen Zugriffe von außen wird durch Firewalls reguliert und erfolgt standardmäßig über eine Sicherheitsinfrastruktur-Kette aus Proxy, Virenscanner und Firewall. An einigen Standorten kann hierfür die spezielle Rolle des Network Security Officer zuständig sein.

Es ist möglich ein Intrusion Prevention System (IPS) zur aktiven Bekämpfung von Netzwerkangriffen (Remote Access, Access Control-Listen, spezielle WAN Bereiche, etc.) zur Verfügung zu stellen, welches nach Beauftragung im Leistungsschein für die unterschiedlichen Verarbeitungen definiert und eingepreist wird.

3.2.2.3 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

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 werden. 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.

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

3.2.2.4 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 über interne Richtlinien angewiesen, nur sichere Datenübertragungswege zu nutzen. Die mögliche Datenübertragung kann über vertrauenswürdige Leitungen und Netze, welche ein Mitprotokollieren nicht ohne Weiteres ermöglichen, erfolgen.

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, können auf Anfrage umgesetzt und in den Leistungsscheinen dokumentiert und bewertet werden.

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.

Für die Sicherung (Backup) von Daten werden bewegliche Datenträger und VTL-Libraries genutzt, welche einer automatischen Inventarisierung unterworfen sind und in einem Sicherheitsbereich lagern.

Zur Gewährleistung einer Transportkontrolle erfolgt ein Transport oder Versand von Datenträgern nur, wenn dieser vom Auftraggeber angewiesen wurde. Dieser bestimmt ebenfalls den Transportweg, welcher beispielsweise der Versand per Einschreiben/Wertpaket oder die Verwendung gesicherter/verschlossener Transportbehältnisse sowie spezieller Kurierdienste (verschlüsselter Versand) umfasst. Dieses unterliegt einem Kontroll- und Dokumentationsprozess.

Eine notwendige Vernichtung von Datenträgern erfolgt durch ein spezialisiertes und zertifiziertes Unternehmen nach aktuellen Normen. 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 in der Informationssicherheitsrichtlinie. Diese stellen sicher, dass personenbezogene Daten oder Betriebs- und Geschäftsunterlagen auf mobilen Datenträgern nur verschlüsselt abgelegt werden dürfen. Dieses verhindert im Rahmen der Datenträgerkontrolle das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern.

Für die sichere Vernichtung bzw. die Entsorgung von Datenträgern und vertraulicher Dokumente existieren Verhaltensregeln.

3.2.2.5 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. Die unterschiedlichen Optionen werden im Leistungsschein für die unterschiedlichen Verarbeitungen definiert und bewertet.

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

Bei einer Tätigkeit per Remote-Zugriff greift der Mitarbeiter auf die bereits vorgegebene Infrastruktur zu, welche ihm eine Verarbeitung im Rahmen der vorher festgelegten Vorgaben ermöglicht.

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

3.2.3.1 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 im Rahmen des Leistungsscheines definiert werden.

Administrative Zugriffe auf Systeme können durch ein Standard-Logging auf Betriebssystemebene nachvollzogen werden. Dieses dient zum Nachweis einer unbefugten Veränderung oder Löschung von gespeicherten personenbezogenen Daten im Rahmen der Speicherkontrolle.

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

3.2.3.2 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.

Eine Konkretisierung ist im jeweiligen Leistungsschein aufzunehmen.

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

3.2.4.1 Verfügbarkeitskontrolle

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

Sämtliche Einrichtungen des Data Centers sind physisch gegen Sicherheitsbedrohungen und Umweltgefahren geschützt.

Unterschiedliche abgestufte Sicherheitseinrichtungen, zur Sicherstellung der Verfügbarkeit, können für das Geschäftsmodell im Leistungsschein definiert und konkretisiert werden.

Hier einige Möglichkeiten: redundante Stromzuführung, hochverfügbare Stromversorgung (teilweise 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 Data Center 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).

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

Optional ist eine Zusammenarbeit mit externen Data Center über Sub-Dienstleister möglich, diese stehen für den Testbetrieb, Redundanz-Konzepte (Geo-Redundanz) auf Anwendungsebene (durch Cluster, Trennung Data Center, separate Daten-Spiegel etc.) auf Weisung zur Verfügung.

Für ein vollumfängliches Backup, je nach Zweckbindung der jeweiligen Verarbeitung, stehen unterschiedliche Archivierungsmöglichkeiten zur Verfügung, z.B. eine regelmäßige automatisch initiierte und

überwachte Datensicherung (üblicherweise einmal pro Kalenderwoche eine Vollsicherung, tägliche inkrementelle Sicherungen). Die normale Haltezeit dieser Sicherungen wird auf Weisung umgesetzt und im Leistungsschein dokumentiert. Die Datensicherung kann in einem separaten Backup-System, welches in einem anderen Brandschutzabschnitt oder an einem anderen Standort wie das Produktivsystem steht, erfolgen.

Auf allen Arbeitsplatzrechnern der Arvato Systems kommt ein Virenschutz zum Einsatz. Das Vorhandensein eines Virenschutzes, sowie die regelmäßige Aktualisierung des Virenpatterns wird durch den Einsatz einer zentralgesteuerte Client-Antivirus-/ und Firewall-Lösung sichergestellt.

Das zeitnahe Einspielen von Sicherheitsupdates für die genutzten Betriebssysteme und Anwendungsprogramme wird über entsprechende Group Policies vorgeschrieben und durch Überwachung des Patch-Levels sichergestellt.

Themen rund um das BCM (Business Continuity Management) sind in dem Kapitel Incident-Response-Management genauer beschrieben.

3.2.4.2 Auftragskontrolle

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

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 nach Spezialverpflichtungen wie z.B. das Fernmeldegeheimnis, das Sozialgeheimnis und das Postgeheimnis verpflichtet. Eine Einsichtnahme ermöglicht die Durchführung von stichprobenartigen Kontrollen.

Data Center-Besichtigungen oder Audits sind in den relevanten Data Center nach der Verhältnismäßigkeit und rechtzeitiger schriftlicher Anmeldung beim verantwortlichen Fachbereich möglich.

Die Organisation und Durchführung eines Audits unterliegt, zum Schutz der personenbezogenen Daten unterschiedlicher Verantwortlicher, der Auditrichtlinie.

3.2.5 Allgemeingültige Verfahren bei Arvato Systems zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

3.2.5.1 Datenschutzmanagement bei der Arvato Systems Group

Für sämtliche rechtliche Einheiten der Arvato Systems, in denen das Kerngeschäft 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 externer Datenschutzbeauftragter bestellt, soweit dieses vom Gesetz vorgegeben ist. Als Ansprechpartner in den einzelnen rechtlichen Einheiten steht ein Team aus ausgebildeten Datenschutzbeauftragten, in der Funktion von Datenschutzkoordinatoren, unter der E-Mailadresse Datenschutz@arvato-systems.de, zur Verfügung.

Arvato Systems definiert die Eckpfeiler des Datenschutzes in der Konzerndatenschutzrichtlinie, sowie konkreter in der Arvato Systems internen Datenschutzrichtlinie.

Durch die IT-Revision und den Datenschutzbeauftragten (falls bestellt) werden in regelmäßigen Abständen Audits zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen durchgeführt. Im Rahmen der Verhältnismäßigkeit besteht nach rechtzeitiger Vorankündigung eine Kontrollmöglichkeit im Rahmen eines Audits durch den Auftraggeber.

Als Nachweis, für eine sicherheitsrelevante Verarbeitung, kann Arvato Systems Zertifikate nachweisen. Sie finden die Zertifikate unter folgendem Link: arvato-systems.de/zertifizierungen

Bei Arvato Systems kann ein ISAE-Report zum Nachweis einer ordnungsgemäßen Verarbeitung und der Beachtung der Informationssicherheit erworben werden.

Das Sicherheitskonzept der Arvato Systems ist in der Konzernrichtlinie zur Information-Security-Policy festgeschrieben.

Zur Erhöhung des Schutzniveaus bei der Verarbeitung von personenbezogenen Daten für den Betroffenen ist die interne Datenschutzrichtlinie der Arvato Systems-Group* mit genehmigten Verhaltensregeln für alle Mitarbeiter einzuhalten. Ebenfalls wird das Risiko durch ein wirksames Patch-Management, Pentests, Log-Analysen, Beschäftigung mit Websicherheit (z.B. OWASP) und über ein Security Operations Center gewährleistet. Für die technischen und organisatorischen Maßnahmen wird ein risikobasierter Ansatz präferiert.

Die Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und 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).

3.2.5.2 Incident-Response-Management bei der Arvato Systems Group

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

Im Rahmen des etablierten BCM (Business Continuity Management) zur Sicherstellung des Geschäftsbetriebes während einer Notlage oder Großstörung sowie zur schnellstmöglichen Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste sind Verfahren dokumentiert. Es werden regelmäßig Wiederanlauf-Übungen durchgeführt.

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 im Abschnitt Verfügbarkeitskontrolle detaillierter aufgenommen.

3.2.5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) bei der Arvato Systems Group

Die Umsetzung des Datenschutzes wird bei der Produktentwicklung durch die Berücksichtigung eines internen White Paper „Datenschutz in der Produktentwicklung“, sowie einer internen Checkliste zur Berücksichtigung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen begleitet.

4 Verarbeitungskategorie: Data Center Public Cloud

Data Center Public Cloud

4.1 Definition Data Center Public Cloud

In der Verarbeitungskategorie „Data Center Public Cloud“ fasst die Arvato Systems-Gruppe* alle Verarbeitungen und Dienstleistungen für ihre Auftraggeber zusammen, die im Zusammenhang mit der Bereitstellung und Wartung von Servern, Storage, Netzwerken oder anderer Data Center-Infrastruktur stehen, die sich in einem **von Arvato Systems beauftragten** externen Public Cloud Data Center befinden. Dieses geschieht in Zusammenarbeit mit externen öffentlichen Cloud-Infrastruktur-Anbietern wie z.B. Amazon Web Services, Microsoft oder Google.

Diese Verarbeitungskategorie dient dazu, dem Auftraggeber eine räumliche Einordnung seines Datenflusses zu ermöglichen.

4.2 Technische und organisatorische Maßnahmen der Data Center Public Cloud Anbieter

In diesem Kapitel finden sie die Links zu den technischen und organisatorischen Maßnahmen (im Folgenden TOM) der großen Public Cloud Anbieter aufgeführt welche für Ihr Geschäftsmodell zutreffen könnten. Hiermit ist es dem Auftraggeber möglich sich direkt über die aktuellen TOM zu informieren, welche im Vertrag zur Auftragsverarbeitung aufgeführt sind und dem jeweiligen Geschäftsmodell zugrunde liegen.

4.2.1 Amazon Web Services

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

4.2.2 Microsoft

Überblick:
https://www.microsoft.com/de-de/trustcenter/privacy/privacy-overview

Dokument:
https://www.microsoft.com/en-us/download/details.aspx?id=55710

4.2.3 Google

https://cloud.google.com/security/privacy/?hl=de

4.2.4 Oracle

https://www.oracle.com/de/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html

4.2.5 SAP

https://www.sap.com/germany/about/cloud-trust-center/cloud-service-level-agreements/cloud-services.html?search=Data Processing&sort=title_asc

5 Verarbeitungskategorie: Data Center Customer

5.1 Definition Data Center Customer

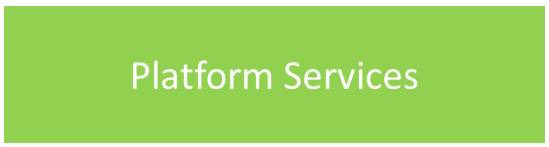
Sollten die Daten oder die Hardware des Auftraggebers in einem vom Auftraggeber verantworteten oder beauftragten Data Center liegen, so gelten für die Bereitstellung dieser Data Center-Infrasturktur ausschließlich die TOMs des jeweiligen Data Center des Auftraggebers. Der Auftraggeber ist für die TOMs und deren Ausprägung vollumfänglich verantwortlich.

Diese Verarbeitungskategorie dient dazu, dem Auftraggeber eine räumliche Einordnung seines Datenflusses zu ermöglichen.

5.2 Technische und organisatorische Maßnahmen der Data Center Customer

Der Auftraggeber definiert seine TOMs und ist für deren Ausprägung vollumfänglich verantwortlich.

6 Verarbeitungskategorie: Platform Services



6.1 Definition Platform Services

Die Verarbeitungskategorie „Platform Services“ beinhaltet alle Verarbeitungen im Zusammenhang mit der Systemadministration von IT-Komponenten, der Inbetriebnahme, Konfiguration, Wartung und des Betriebes von Basis-Softwarekomponenten (in einem Data Center und für die darauf aufsetzenden IT-Applikationen) wie z.B. von Datenbanken, SAP-Basis, SharePoint-Farmen, Firewalls und Virenscannern oder Backup- und Recovery-Services.

6.2 Technische und organisatorische Maßnahmen der Platform Services

Für diese Verarbeitungskategorie gelten die allgemeingültigen technischen und organisatorischen Maßnahmen der Arvato Systems Gruppe* (siehe Kapitel 2) und die technischen und organisatorischen Maßnahmen der jeweils relevanten Data Center (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer).

7 Verarbeitungskategorie: Applikation Management & Services

7.1 Definition Application Management & Services

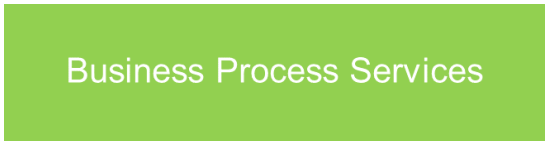
Die Verarbeitungskategorie „Application Management & Services“ umfasst alle Verarbeitungen im Zusammenhang mit dem kompletten Life Cycle von IT-Applikationen. Enthalten sind hier einerseits die Applikationsentwicklung (Analyse, Konzeption, Entwicklung und Test) von IT-Applikationen und andererseits der Applikationsbetrieb (Inbetriebnahme, Aufrechterhaltung des Betriebes und Wartung) von IT-Applikation durch Arvato Systems.

Je nach Beauftragung fallen hierunter auch weitere Support- und Serviceleistungen von Arvato Systems im Zusammenhang mit der IT-Applikation wie z.B. die Anwenderbetreuung, die Administration von Berechtigungen, die Erstellung von Auswertungen / Reports, Datenanalysen oder -migrationen gemäß den Vorgaben des Auftraggebers.

7.2 Technische und organisatorische Maßnahmen der Application Management & Services

Für diese Verarbeitungskategorie gelten die allgemeingültigen technischen und organisatorischen Maßnahmen der Arvato Systems Gruppe* (siehe Kapitel 2) und die technischen und organisatorischen Maßnahmen der jeweils relevanten Data Center (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer).

8 Verarbeitungskategorie: Business Process Services



8.1 Definition Business Process Services

Gegenstand der „Business Process Services“ ist die Durchführung und Unterstützung von IT-gesteuerten Geschäftsprozessen des Auftraggebers durch Arvato Systems z.B. Newsletterversand oder Callcenter-Tätigkeiten. Dieses wird durch den Einsatz von Arvato Systems-Mitarbeitern oder beauftragten Dienstleistern ermöglicht.

8.2 Technische und organisatorische Maßnahmen der Business Process Services

Für diese Verarbeitungskategorie gelten die allgemeingültigen technischen und organisatorischen Maßnahmen der Arvato Systems Gruppe* (siehe Kapitel 2) und die technischen und organisatorischen Maßnahmen der jeweils relevanten Data Center (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer).

9 Verarbeitungskategorie: Workplace Services

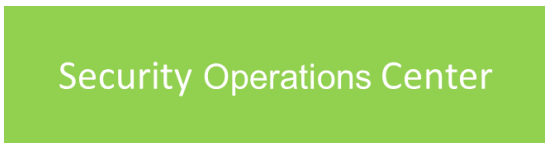
9.1 Definition Workplace Services

Die Verarbeitungskategorie „Workplace Services“ umfasst alle Verarbeitungen im Zusammenhang mit der Bereitstellung, Verwaltung und Betreuung von IT-gestützten Arbeitsplätzen des Auftraggebers. Hierunter fallen die Bereitstellung und (Software-)Konfiguration von PCs, Notebooks, Druckern oder mobilen Endgeräten durch die Arvato Systems-Gruppe* sowie die Bereitstellung eines Kundenservices für Nutzeranfragen aber z.B. auch das Identitätsmanagement oder der Betrieb und die Administration von Verzeichnisdiensten, Fileservern oder Mobil Device Management Lösungen. Darüber hinaus fallen unter diese Verarbeitungskategorie auch Mail & Collaboration-Services wie die Administration von E-Mail-, Messaging-, Chat- oder Sprach-Diensten oder Telefonanlagen in Kooperation mit unterschiedlichen Technologiepartnern, insbesondere auch im Office 365-Umfeld.

9.2 Technische und organisatorische Maßnahmen der Workplace Services

Für diese Verarbeitungskategorie gelten die allgemeingültigen technischen und organisatorischen Maßnahmen der Arvato Systems Gruppe* (siehe Kapitel 2) und die technischen und organisatorischen Maßnahmen der jeweils relevanten Data Center (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer).

10 Verarbeitungskategorie: Security Operations Center



10.1 Definition Security Operations Center

Verarbeitungen der Verarbeitungskategorie „Security Operations Center“ umfassen Services, die je nach Beauftragung den Auftraggeber dabei unterstützen, seine Netze und Systeme gegen die verschiedenen Formen von Cyber-Bedrohungen zu schützen.

Es werden gemäß des Defense in Depth-Ansatzes Services für Protection, Detection und Reaction angeboten. Durch Analyse des Netzwerk-Traffics oder Log-Daten werden Angriffe erkannt (Detection), auf welche geordnet reagiert werden kann (Reaction). Monitoring von Sicherheitstools und professionelles Vulnerability Management (Protection) erhöhen die Netzwerksicherheit.

Diese Services sichern die Infrastruktur des Auftraggebers im Data Center von Arvato Systems, im eigenen Data Center des Auftraggebers sowie in der Cloud Infrastruktur, je nach Beauftragung.

Ebenfalls fallen hierunter Netzwerk Sicherheitsdienste wie Security Consulting, Schwachstellen-Scan-Services oder aktives Security-Monitoring mit einem Security Information and Event Management (SIEM), etc.

10.2 Technische und organisatorische Maßnahmen der Security Operations Center

Für diese Verarbeitungskategorie gelten die allgemeingültigen technischen und organisatorischen Maßnahmen der Arvato Systems Gruppe* (siehe Kapitel 2) und die technischen und organisatorischen Maßnahmen der jeweils relevanten Data Center (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer).

11 Arvato Systems Gruppe

*Die Arvato Systems Gruppe ist unter der E-Mail-Adresse: info@arvato-systems.de zu erreichen und umfasst die folgenden Gesellschaften:

- Arvato Systems GmbH, An der Autobahn 20, 33333 Gütersloh, Deutschland
- Arvato Systems Perdata GmbH, Martin-Luther-Ring 7-9, 04109 Leipzig, Deutschland
- Arvato Systems S4M GmbH, Am Coloneum 3, 50829 Köln, Deutschland
- Next Level Integration GmbH, Nattermannallee 1, 50829 Köln, Deutschland
- Arvato Systems Latvia SIA, Zaļā iela, Centra rajons, Rīga, LV-1010, Lettland
- Vidispine AB, Kista Alléväg 3, 164 55 Kista, Sweden
- Arvato Systems IT S.R.L., Brasov Business Park, Strada Ionescu Crum Nr.1, 500446 Brasov, Romania.
- Arvato Systems North America, Inc., 1745 Broadway, 20th Floor, New York, NY 10019
- Arvato Systems Malaysia Sdn Bhd (707776-M), Anschrift: Suite 26-10, Level 26, GTower, 199, Jalan Tun Lumpur, 50400 Kuala Lumpur, Malaysia