Anhang TOM

Technische und organisatorische Mindestmaßnahmen

für Dienstleister von Arvato Systems

Version 4.0

Öffentlich

Disclaimer

Inhaltsverzeichnis

1 Vereinbarung konkreter technischer und organisatorischer Maßnahmen

Die vom Auftragnehmer konkret implementierten technischen und organisatorischen Maßnahmen ergeben sich aus

- dem Hauptvertrag inklusive aller Anlagen wie z.B. den Leistungsbeschreibungen des Hauptvertrages sowie ergänzend
- den technischen und organisatorischen Mindestmaßnahmen in Abschnitt 2, wobei der jeweils anwendbare Typ des Zugangs (siehe 1.1) aus dem Hauptvertrag abzuleiten ist.

1.1 Definition Typ des Zugangs

Die Menge der minimal zu erfüllenden Maßnahmen hängt von dem Typ des Zugangs des Auftragnehmers auf Daten des Auftraggebers ab. Der Typ des Zugangs wird in folgender Tabelle definiert.

Typ	Kurzbeschreibung des Typs	Definition des Typs des Zugangs
A	Auftragnehmer erbringt eine Kernleistung auf eigenen IT-Systemen	Der Zugang zu Daten des Auftraggebers fällt weder in den Typ B, noch C, noch D.
B	Auftragnehmer erhält Zugang zu von Arvato Systems bereitgestellten IT-Systemen über Endgeräte des Auftragnehmers	Zur Erbringung der Leistung erhält der Auftragnehmer Zugang zu vom Auftraggeber bereitgestellten IT-Systemen und nutzt zum Zugang Endgeräte des Auftragnehmers. Es findet keine Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers auf IT-Systemen des Auftragnehmers außerhalb der Endgeräte statt.
C	Auftragnehmer erhält Zugang zu von Arvato Systems bereitgestellten IT-Systemen über Endgeräte von Arvato Systems	Zur Erbringung der Leistung erhält der Auftragnehmer Zugang zu vom Auftraggeber bereitgestellten IT-Systemen und nutzt zum Zugang Endgeräte des Auftraggebers. Es findet keine Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers auf IT-Systemen des Auftragnehmers statt.
D	Auftragnehmer erhält nur Logdaten ohne Zugang zu Arvato Systems IT-Systemen	Nur Auszüge pseudonymisierter Meta-/Logdaten normaler Schutzstufe von IT-Systemen des Auftraggebers werden an den Auftragnehmer übermittelt um die Vertraulichkeit, Verfügbarkeit, Integrität oder Belastbarkeit der IT-Systeme sicherzustellen. Der Auftragnehmer erhält keinen Zugang zu IT-Systemen des Auftraggebers.

2 Technische und organisatorische Mindestmaßnahmen

Folgende technische und organisatorische Maßnahmen sind Mindeststandards für die Verarbeitung von personenbezogenen Daten im Auftrag des Auftraggebers und gelten für Assets, Systeme und Prozesse, für die der Auftragnehmer Owner ist oder im Vertrag als „accountable (= verantwortet die Leistung bzw. trifft damit zusammenhängende Entscheidungen“) festgelegt ist.

2.1 Mindestmaßnahmen

In der folgenden Tabelle werden die geforderten Mindestmaßnahmen je Typ des Zugangs (siehe Definition 1.1 für Typ A, B, C oder D) aufgelistet. Werden Tätigkeiten zur Leistungserbringung vom Auftragnehmer auch aus dem Homeoffice oder durch mobiles Arbeiten erbracht, so sind zusätzlich die Maßnahmen im Kap. 2.2 zu erfüllen.

Nr.	Maßnahme	A	B	C	D
1. Organisation des Datenschutzes und der Informationssicherheit					
1.1	Es existieren Regelwerke für Informationssicherheit und Datenschutz.	x			x
1.2	Die Regelwerke für Informationssicherheit und Datenschutz werden regelmäßig auf Einhaltung und Wirksamkeit geprüft.	x			x
1.3	Die Sicherheitskonzepte und -maßnahmen und deren Implementierung werden regelmäßig überprüft.	x	x	x	x
1.4	Es ist eine Person benannt, die für die Einhaltung dieser technischen und organisatorischen Sicherheitsmaßnahmen insgesamt verantwortlich ist.	x	x	x	x
2. Personalsicherheit					
2.1	Mitarbeitende durchlaufen einen Starter-Changer-Leaver Prozess, der Sicherheitsanforderungen bei Stellenbesetzung, -wechsel und -beendigung berücksichtigt.	x	x	x	x
2.2	Mitarbeitende werden auf das Datenschutzgeheimnis verpflichtet.	x	x	x	x
2.3	Mitarbeitende werden regelmäßig zu Datenschutz und Informationssicherheit geschult.	x	x	x	x
2.4	Anweisungen für die Handhabung, Verarbeitung und Weiterleitung von Informationen, den Umgang mit mobilen Endgeräten und Speichermedien sowie die Gestaltung von Arbeitsumgebungen sind festgelegt (acceptable use policy, clean desk policy).	x	x	x	x
3. Assetmanagement					
3.1	Verfahren zur Inventarisierung der Assets und zur Führung des Verzeichnisses der Verarbeitungstätigkeiten sind definiert und eingeführt.	x	x		x
3.2	Vorgaben zur Klassifizierung von Daten in verschiedene Schutzklassen sind etabliert.	x			x
3.3	Transporte von Datenträgern mit personenbezogenen Daten unterliegen einem Kontroll- und Dokumentationsprozess und werden bei Transport außerhalb des Bereiches des Unternehmens in gesicherten, verschlossenen Transportbehältnissen durch spezielle Kurierdienste transportiert oder mit Verfahren wie Verschlüsselung gesichert.	x			x
3.4	Verfahren zur Entsorgung von Geräten, Datenträgern und vertraulichen Dokumenten sind eingeführt, die auch Vorgaben für die Löschung von Informationen bzw. die Vernichtung durch spezialisierte und zertifizierte Unternehmen nach aktuellen Normen enthält.	x	x		x
4. Physische und umgebungsbezogene Sicherheit					
4.1	Physische Sicherheitskontrollen für Büros, Räume und Einrichtungen sind konzipiert und umgesetzt.	x	x		x
4.2	Es existiert ein dokumentiertes Verfahren zur Vergabe, Änderung und Entzug von Zutrittsrechten inkl. Rückgabe der Zutrittsmittel.	x	x		x
4.3	Sicherheitsbereiche (Bereiche mit höheren Sicherheitsanforderungen) sind festgelegt, in Sicherheitszonen unterteilt und zusammen mit den physischen Schutzmaßnahmen in einem Sicherheitszonenkonzept dokumentiert.	x			x
4.4	Sicherheitsbereiche sind in Abhängigkeit von der Sicherheitszone durch angemessene Zutrittskontrollen und physische Barrieren gemäß dem Sicherheitszonenkonzept geschützt. Der Zutritt zu Sicherheitszonen wird gesteuert und genehmigt, um nur autorisierten Personen Zutritt zu gewähren. Zutrittskontrollen, die Besuchern den Zutritt zu Sicherheitszonen ermöglichen, sind definiert.	x			x
4.5	Der Zutritt zum Data Center des Auftragnehmers erfolgt nachvollziehbar über ein persönlich zugeordnetes Zutrittsmittel mit Zwei-Faktor-Authentifizierung oder einer vergleichbaren Methode.	x			x
4.6	Alle Besucher der Data Center des Auftragnehmers werden mit Datum und Uhrzeit ihres Betretens und Verlassens erfasst und durch autorisiertes Personal begleitet.	x			x

Nr.	Maßnahme	A	B	C	D
4.7	Data Center des Auftragnehmers sind physisch gesichert, mit Einbruchmeldeanlagen geschützt und Eingänge werden mit Videoanlagen überwacht.	x			x
4.8	In den Data Centern vom Auftragnehmer sind Schutzmaßnahmen gegen technische Beeinträchtigungen und elementare Umweltgefährdungen - insb. Feuer, Wasser, Ausfall von Versorgungsnetzen - vorhanden (wie z.B. USV, Notstromanlage, Feuerlöscher, Branderkennung etc.). Abweichungen vom Normalbetrieb lassen sich schnell aufspüren und beheben.	x			x
4.9	Data Center Infrastruktur des Auftragnehmers wird gemäß den Herstellerspezifikationen gewartet.	x			x
4.10	Physische Geräte und Serversysteme befinden sich in einer Sicherheitszone, die ihren Schutzanforderungen entspricht.	x			x
5. Zugangssteuerung					
5.1	Im Rahmen des Identity & Access Managements sind Prozesse zur Vergabe, Änderung und zum Entzug von Zugangs- und Zugriffsrechten dokumentiert und vorhanden.	x			x
5.2	Vorgänge zur Vergabe oder Änderung von Zugangs- und Zugriffsrechten sind nachvollziehbar dokumentiert und vom zuständigen Genehmiger freigegeben.	x			x
5.3	Jeder Account ist immer eindeutig einer natürlichen Person zugeordnet.	x			x
5.4	Accounts und Zugangsdaten können unverzüglich gesperrt werden.	x			x
5.6	Es sind Maßnahmen zum Schutz der Benutzer/Passwort Authentifizierung implementiert.	x	x		x
5.7	Es werden Passwörter mit ausreichender Komplexität und Länge verwendet. Aufbau und Handhabung von Passworten erfolgt gemäß einer dokumentierten Passwortrichtlinie.	x	x	x	x
5.8	Default Passwörter werden sofort nach der Installation geändert. Initial-Passwörter sind individualisiert.	x			
5.9	Für Administrator-Tätigkeiten werden gesonderte Accounts/Rollen und Zugangsdaten vergeben. Administrator-Accounts dürfen nicht für normale Bürotätigkeiten verwendet werden.	x			x
5.10	Die Durchführung von Administrator-Tätigkeiten mit privilegierten Zugangsrechten im Data Center des Auftragnehmers erfolgt über Sprungserver, virtuelle Desktops im Data Center sowie ein PAM (Privileged Access Management) System.	x			
5.11	Standardmäßig werden Geräte und Sitzungen nach einer bestimmten Zeit der Inaktivität automatisch gesperrt.	x	x		x
5.12	Alle Zugänge zu Systemen (Mobile Endgeräte, Applikationen, Betriebssystemen, BIOS, Boot-Devices etc.) sind gesichert oder gesperrt.	x	x		x
6. Zugriffssteuerung					
6.1	Es werden nur die Zugriffsrechte vergeben, die zur Erfüllung der jeweiligen Aufgabenstellung erforderlich sind (need-to-know und least-privilege Prinzip).	x			x
6.2	Erteilte Zugriffsrechte werden in regelmäßigen Abständen überprüft, die sich nach der Kritikalität der betreffenden Zugriffsrechte richten. Für besonders kritische Accounts ist eine aktive Neugenehmigung erforderlich. Zugriffsrechte werden unverzüglich entzogen, sofern sie nicht mehr erforderlich sind.	x			x
6.3	In allen Systemen/Applikationen sind rollenbasierte Berechtigungskonzepte implementiert.	x			x
7. Verschlüsselung					
7.1	Daten auf mobilen Endgeräten sind entsprechend dem Stand der Technik verschlüsselt und vor unerkannter Manipulation geschützt.	x	x		x

Nr.	Maßnahme	A	B	C	D
7.2	Daten werden bei Transport über öffentliche Netze gegen unbefugte Offenlegung und Manipulation geschützt. (z. B. Transportverschlüsselung über TLS).	x	x	x	x
7.3	Zur Unterstützung kryptographischer Maßnahmen und Techniken wird ein geeignetes kryptographisches Schlüsselmanagement implementiert.	x			
7.4	Implementierte kryptografische Techniken entsprechen Best Practices. Unsichere (veraltete) Techniken werden zeitnah ersetzt.	x			x
7.5	Die Vorgaben zur Verschlüsselung der Daten werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und in den Leistungsscheinen konkretisiert.	x			
7.6	Sofern angemessen, werden data-at-rest verschlüsselt.	x			x
8. Pseudonymisierung					
8.1	Die Vorgaben zur Pseudonymisierung werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und in den Leistungsscheinen konkretisiert.	x			
9. Betrieb					
9.1 Betrieb - Änderungssteuerung					
9.1.1	Bestandteil einer neuen oder zu ändernden Verarbeitungstätigkeit ist eine Bewertung der Risiken der Betroffenen und davon abhängig die Identifikation und Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen.	x			x
9.1.2	Die IT-Betriebsverfahren sind nachvollziehbar dokumentiert, werden regelmäßig geprüft und bei Bedarf angepasst.	x			
9.1.3	Änderungen an Informationsverarbeitungssystemen unterliegen einem Change-Management Prozess.	x			x
9.1.4	Regeln für die Softwareinstallation und Konfiguration durch Benutzer sind festgelegt, werden umgesetzt und überwacht.	x			x
9.1.5	Um das Risiko des Missbrauchs von Assets zu verringern, sind die Freigaben und die Ausführung der operativen Verfahren in verschiedenen Rollen getrennt.	x			x
9.2 Betrieb - Trennungskontrolle					
9.2.1	Personenbezogene Daten von Auftraggebern werden so verarbeitet, dass der Auftraggeber in der Verarbeitung identifiziert werden kann. Somit sind die Daten verschiedener Auftraggeber immer physisch oder logisch getrennt.	x			x
9.2.2	Entwicklungs-, Test- und Produktivumgebungen sind getrennt.	x			x
9.3 Betrieb - Schutz vor Malware und Vulnerabilities, Patchmanagement					
9.3.1	Auf allen relevanten Informationssystemen und mobilen Endgeräten ist ein aktueller Schutz vor Malware und bösartigen Aktivitäten installiert und aktiviert.	x	x		x
9.3.2	Für alle Systeme werden neue Sicherheitsupdates und -patches zeitnah eingespielt, wobei Systemabhängigkeiten, die Auswirkungen auf den laufenden Betrieb sowie die Schadensauswirkungen einer Schwachstelle und die Bedrohungslage berücksichtigt werden.	x	x		x
9.3.3	Software wird gemäß festgelegter Konfigurations- und Härtungsstandards installiert.	x	x		x
9.3.4	Informationen über technische Schwachstellen verwendeter Informationssysteme werden eingeholt. Für alle Systeme wird die Gefährdung durch Schwachstellen je nach Kritikalität des Systems regelmäßig bewertet. Geeignete Abhilfemaßnahmen werden ergriffen, um einer Ausnutzung technischer Schwachstellen entgegenzuwirken.	x			x

Nr.	Maßnahme	A	B	C	D
9.3.5	Penetrationstests werden in bestimmten Abständen geplant und durchgeführt, je nach Kritikalität und Gefährdung der betroffenen Systeme.	x			
9.4 Betrieb - Verfügbarkeit					
9.4.1	Die Vorgaben zur Verfügbarkeit der Auftraggeber-Daten (Datensicherung, redundante Systeme, Geo-redundante Data Center, etc.) werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und in den Leistungsscheinen konkretisiert.	x			
9.4.2	Datensicherungs- und Wiederherstellbarkeitsverfahren werden regelmäßig getestet, insbesondere nach Änderungen der Sicherungskonfiguration.	x			
9.4.3	Ein Prozess zum Test redundanter Systeme im Hinblick auf die Verfügbarkeitsanforderungen ist eingerichtet.	x			
9.5 Betrieb - Netzwerk					
9.5.1	Das Netzwerk des Auftragnehmers wird in geeigneter Weise verwaltet, um die Informationen in Systemen und Anwendungen zu schützen. Es ist in verschiedene Zonen unterteilt.	x	x		x
9.5.2	Der externe Zugriff (Fernzugriff) auf die Netzwerke und Systeme des Auftragnehmers ist geschützt und verschlüsselt und verlangt eine Zwei-Faktor-Authentifizierung.	x			
9.5.3	Nur ausreichend geschützte mobile Endgeräte erhalten Zugriff auf das Netzwerk des Auftragnehmers.	x			
9.6 Betrieb - Protokollierung und Überwachung					
9.6.1	Logs, die Aktivitäten (inkl. Administrative Tätigkeiten), Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, werden erstellt und gespeichert. Der Detaillierungsgrad der Logs richtet sich nach der Sensibilität der Informationen und der Kritikalität des Systems und ermöglicht Eingaben und Änderungen personenbezogener Daten nachzuvollziehen.	x	x		
9.6.2	Netzwerk-Traffic zwischen den Netzwerkzonen wird geloggt und überwacht.	x			
9.6.3	Auf den Notebooks erzeugte Ereignis-Meldungen zur Erkennung von Informationssicherheitsvorfällen werden zur Auswertung an zentrale Server übermittelt.	x			
9.6.4	Log-Systeme und Log-Daten in der Hoheit vom Auftragnehmer werden vor unbefugtem Zugriff, Änderung und Löschung geschützt.	x			
9.6.5	Die Uhren kritischer Systeme werden mit einem zuverlässigen und vereinbarten Zeitserver synchronisiert.	x			
9.6.6	Der Grad der Überwachung von System- und Netzwerkressourcen wird einer Risikobewertung entsprechend festgelegt.	x	x		x
9.6.7	Rollen und Verantwortlichkeiten zum Schutz vor Cyber-Threads sind definiert und umgesetzt (Security Operations Center). Log-Daten werden auf Sicherheitsereignisse analysiert.	x			
10. Anschaffung, Entwicklung und Instandhaltung von IT-Systemen					
10.1	Es gibt Vorgaben zur Softwareentwicklung und Anschaffung von IT-Systemen und IT-Services, die die Aspekte der IT-Sicherheit und des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen beinhalten.	x			x
11. Lieferantenmanagement					
11.1	Vereinbarungen mit Unterauftragnehmern über den Austausch von Informationen werden abgeschlossen und berücksichtigen die Sicherheit der Daten.	x	x	x	x
11.2	Vor der Beauftragung externer Unterauftragnehmer erfolgt eine Bewertung der Datenschutz- und Informationssicherheits-Risiken in Bezug auf ihre zukünftigen Aufgaben. Die Auswahl eines geeigneten Unterauftragnehmers basiert auf den Ergebnissen dieser Bewertung.	x	x	x	

Nr.	Maßnahme	A	B	C	D
11.3	Die Einhaltung der Auftragsverarbeitungsverträge wird regelmäßig bewertet und überprüft.	x	x	x	x
12. Handhabung von Sicherheits- und Datenschutzvorfällen					
12.1	Prozesse zur Identifikation, Bewertung und Handhabe von Sicherheits- und Datenschutzvorfällen sind eingeführt und geschult.	x			x
12.2	Zentrale Stellen sind für die Koordinierung und Reaktion auf Informationssicherheits- und Datenschutzvorfälle zuständig, führen die Bewertung durch und entscheiden über die Klassifizierung der Vorfälle.	x			
12.3	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.	x	x	x	x
13. Business Continuity Management					
13.1	Es gibt ein dokumentiertes Verfahren für das Business Continuity Management. Es sind Prozesse und Zuständigkeiten für die Durchführung des Krisenmanagements festgelegt und es finden regelmäßig entsprechende Übungen statt.	x			x

2.2 Mindestmaßnahmen für mobiles Arbeiten oder Homeoffice

In der folgenden Tabelle werden die über Kap. 2.1 hinaus geforderten Mindestmaßnahmen aufgelistet, die zu erfüllen sind, wenn vom Auftragnehmer Tätigkeiten zur Leistungserbringung aus dem Homeoffice oder durch mobiles Arbeiten erbracht werden.

Nr.	Maßnahme	A	B	C	D
2. Personalsicherheit					
2.5	Mitarbeitende sind angewiesen und geschult, betriebliche Information insbesondere im mobilen Arbeitsumfeld angemessen zu schützen - vor Einsichtnahme unbefugter Dritter auf den Bildschirm durch Blickschutzfolie und Sperrung mobiler Endgeräte bei Nicht-Nutzung - vor Einsichtnahme unbefugter Dritter auf Arbeitsunterlagen/Ausdrucke durch eine Clean Desk Policy - vor Kenntnisnahme unbefugter Dritter von vertraulichen Gesprächen oder Telefonaten - durch angemessen sichere Verwahrung mobiler Endgeräte und Betriebsmittel - durch konforme Entsorgung von Papier und Datenträgern Die Einhaltung der Anweisungen kann durch den Arbeitgeber überprüft werden.	x	x	x	x
5. Zugangssteuerung					
5.4	Accounts und Zugangsdaten können unverzüglich gesperrt werden.	x	x		x
5.5	Konformität der mobilen Endgeräte mit festgelegten Richtlinien wird überwacht. Bei Nicht-Konformität wird der Zugang verweigert.	x			x
5.13	Mitarbeitende nutzen für berufliche Tätigkeiten unternehmensseitig bereitgestellte Hard- und Software inklusive der Standardkommunikationssoftware. Ausnahme beim mobilen Arbeiten: Die für die Internetverbindung erforderlichen Geräte sowie bei Bedarf eigene Peripheriegeräte (z. B. Drucker, Monitor, Maus, Tastatur), wenn diese als gängige Markengeräte aus vertrauenswürdiger Quelle bezogen wurden.	x	x		x
9.5 Betrieb - Netzwerk					
9.5.3	Nur ausreichend geschützte mobile Endgeräte erhalten Zugriff auf das Netzwerk des Auftragnehmers.	x	x		x
9.6 Betrieb - Protokollierung und Überwachung					
9.6.3	Auf den Notebooks erzeugte Ereignis-Meldungen zur Erkennung von Informationssicherheitsvorfällen werden zur Auswertung an zentrale Server übermittelt.	x	x		x