Anhang TOM

Technische und organisatorische Maßnahmen der Arvato Systems Gruppe

Version 4.0

Öffentlich

Disclaimer

Inhaltsverzeichnis

1 Einleitung

In diesem Anhang werden die technischen und organisatorischen Maßnahmen (TOM) der Arvato Systems Gruppe gemäß Art. 32 DSGVO beschrieben.

Alle Verarbeitungen, die Arvato Systems im Auftrag ausführt, sind in Verarbeitungskategorien unterteilt. Diese werden im Abschnitt 4 definiert. Sie unterscheiden sich im Wesentlichen durch den Speicherort:

- Services mit Hosting-Leistungen aus dem Arvato Systems eigenen Data Centern (Data Center Arvato Systems)
- Services mit Hosting-Leistungen auf einer Public Cloud Umgebung, die von Arvato Systems verantwortet wird (Data Center Public Cloud)
- Services, die kein Data Center benötigen oder auf Hosting-Leistungen aufsetzen, die der Auftraggeber selbst bereitstellt (Data Center Customer).

Die vereinbarten Maßnahmen können pro Verarbeitungskategorie unterschiedlich sein.

2 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 allgemeinen technischen und organisatorischen Standardmaßnahmen in Abschnitt 3, wobei die jeweils anwendbaren Verarbeitungskategorien im Auftragsverarbeitungsvertrag vereinbart sind.

Über die vereinbarten Maßnahmen hinaus bietet Arvato Systems weitere Sicherheitsmaßnahmen oder Cyber-Security-Services an, die vom Auftraggeber zusätzlich beauftragt werden können.

Dabei ist zu beachten, dass sich die Sicherheit der Gesamtlösung des Auftraggebers aus den aufeinander abgestimmten technischen und organisatorischen Maßnahmen aller an der Lösung beteiligten Parteien ergibt.

3 Allgemeine technische und organisatorische Standardmaßnahmen

Folgende technische und organisatorische Maßnahmen sind Mindeststandards für Verarbeitungen bei Arvato Systems und gelten für Assets, Systeme und Prozesse, für die Arvato Systems Owner ist oder im Vertrag als „accountable (= verantwortet die Leistung bzw. trifft damit zusammenhängende Entscheidungen“) festgelegt ist.

3.1 Standard-TOM für die Verarbeitungstätigkeiten bei Arvato Systems

Für die folgenden Verarbeitungskategorien gelten die nachstehenden Standard-TOM.

- Business Process Services
- Workplace Services
- Security Operations Center
- Application Management & Services
- Platform Services
- Data Center Arvato Systems
- Data Center Customer

Für jede dieser Verarbeitungskategorien gelten die in der Spalte „generell“ angekreuzten Maßnahmen. Für die Verarbeitungskategorie „Data Center Arvato Systems“ gelten darüber hinaus weitere Maßnahmen, die in der entsprechenden Spalte angekreuzt sind.

Nr.	Maßnahme	generell	Data Center Arvato Systems
1. Organisation des Datenschutzes und der Informationssicherheit			
1.1	Es existieren Regelwerke für Informationssicherheit und Datenschutz.	x	
1.2	Die Regelwerke für Informationssicherheit und Datenschutz werden regelmäßig auf Einhaltung und Wirksamkeit geprüft.	x	
1.3	Die Sicherheitskonzepte und -maßnahmen und deren Implementierung werden regelmäßig überprüft.	x	
2. Personalsicherheit			
2.1	Mitarbeitende durchlaufen einen Starter-Changer-Leaver Prozess, der Sicherheitsanforderungen bei Stellenbesetzung, -wechsel und -beendigung berücksichtigt.	x	
2.2	Mitarbeitende werden auf das Datenschutzgeheimnis verpflichtet.	x	
2.3	Mitarbeitende werden regelmäßig zu Datenschutz und Informationssicherheit geschult.	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	
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	
3. Assetmanagement			
3.1	Verfahren zur Inventarisierung der Assets und zur Führung des Verzeichnisses der Verarbeitungstätigkeiten sind definiert und eingeführt.	x	
3.2	Vorgaben zur Klassifizierung von Daten in verschiedene Schutzklassen sind etabliert.	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	
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	
4. Physische und umgebungsbezogene Sicherheit			
4.1	Physische Sicherheitskontrollen für Büros, Räume und Einrichtungen sind konzipiert und umgesetzt.	x	

Nr.	Maßnahme	generell	Data Center Arvato Systems
4.2	Es existiert ein dokumentiertes Verfahren zur Vergabe, Änderung und Entzug von Zutrittsrechten inkl. Rückgabe der Zutrittsmittel.	x	
4.3	Sicherheitsbereiche (Bereiche mit höheren Sicherheitsanforderungen) sind festgelegt, in Sicherheitszonen unterteilt und zusammen mit den physischen Schutzmaßnahmen in einem Sicherheitszonenkonzept dokumentiert.		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
4.5	Der Zutritt zum Arvato Systems Data Center erfolgt nachvollziehbar über ein persönlich zugeordnetes Zutrittsmittel mit Zwei-Faktor-Authentifizierung oder einer vergleichbaren Methode.		x
4.6	Alle Besucher der Arvato Systems Data Center werden mit Datum und Uhrzeit ihres Betretens und Verlassens erfasst und durch autorisiertes Personal begleitet.		x
4.7	Arvato Systems Data Center sind physisch gesichert, mit Einbruchmeldeanlagen geschützt und Eingänge werden mit Videoanlagen überwacht.		x
4.8	In den Data Centern von Arvato Systems 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
4.9	Arvato Systems Data Center Infrastruktur wird gemäß den Herstellerspezifikationen gewartet.		x
4.10	Physische Geräte und Serversysteme befinden sich in einer Sicherheitszone, die ihren Schutzanforderungen entspricht.	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	
5.2	Vorgänge zur Vergabe oder Änderung von Zugangs- und Zugriffsrechten sind nachvollziehbar dokumentiert und vom zuständigen Genehmiger freigegeben.	x	
5.3	Jeder Account ist immer eindeutig einer natürlichen Person zugeordnet.	x	
5.4	Accounts und Zugangsdaten können unverzüglich gesperrt werden.	x	
5.5	Konformität der mobilen Endgeräte mit festgelegten Richtlinien wird überwacht. Bei Nicht-Konformität wird der Zugang verweigert.	x	
5.6	Es sind Maßnahmen zum Schutz der Benutzer/Passwort Authentifizierung implementiert.	x	
5.7	Es werden Passwörter mit ausreichender Komplexität und Länge verwendet. Aufbau und Handhabung von Passworten erfolgt gemäß einer dokumentierten Passwortrichtlinie.	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	

Nr.	Maßnahme	generell	Data Center Arvato Systems
5.10	Die Durchführung von Administrator-Tätigkeiten mit privilegierten Zugangsrechten im Arvato Systems Data Center 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	
5.12	Alle Zugänge zu Systemen (Mobile Endgeräte, Applikationen, Betriebssystemen, BIOS, Boot-Devices etc.) sind gesichert oder gesperrt.	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	
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	
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	
6.3	In allen Systemen/Applikationen sind rollenbasierte Berechtigungskonzepte implementiert.	x	
7. Verschlüsselung			
7.1	Daten auf mobilen Endgeräten sind entsprechend dem Stand der Technik verschlüsselt und vor unerkannter Manipulation geschützt.	x	
7.2	Daten werden bei Transport über öffentliche Netze gegen unbefugte Offenlegung und Manipulation geschützt. (z. B. Transportverschlüsselung über TLS).	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	
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	
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	
9.1.2	Die IT-Betriebsverfahren sind nachvollziehbar dokumentiert, werden regelmäßig geprüft und bei Bedarf angepasst.	x	

Nr.	Maßnahme	generell	Data Center Arvato Systems
9.1.3	Änderungen an Informationsverarbeitungssystemen unterliegen einem Change-Management Prozess.	x	
9.1.4	Regeln für die Softwareinstallation und Konfiguration durch Benutzer sind festgelegt, werden umgesetzt und überwacht.	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	
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	
9.2.2	Entwicklungs-, Test- und Produktivumgebungen sind getrennt.	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	
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	
9.3.3	Software wird gemäß festgelegter Konfigurations- und Härtungsstandards installiert.	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	
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
9.4.4	Die Auslastung der IT-Ressourcen wird überwacht und an den aktuellen und erwarteten Kapazitätsbedarf angepasst.		x
9.5 Betrieb - Netzwerk			
9.5.1	Das Arvato Systems Netzwerk wird in geeigneter Weise verwaltet, um die Informationen in Systemen und Anwendungen zu schützen. Es ist in verschiedene Zonen unterteilt.	x	
9.5.2	Der externe Zugriff (Fernzugriff) auf die Netzwerke und Systeme von Arvato Systems ist geschützt und verschlüsselt und verlangt eine Zwei-Faktor-Authentifizierung.	x	
9.5.3	Nur ausreichend geschützte mobile Endgeräte erhalten Zugriff auf das Arvato Systems Netzwerk.	x	

Nr.	Maßnahme	generell	Data Center Arvato Systems
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	
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 von Arvato Systems 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	
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	
11. Lieferantenmanagement			
11.1	Vereinbarungen mit Unterauftragnehmern über den Austausch von Informationen werden abgeschlossen und berücksichtigen die Sicherheit der Daten.	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	
11.3	Die Einhaltung der Auftragsverarbeitungsverträge wird regelmäßig bewertet und überprüft.	x	
12. Handhabung von Sicherheits- und Datenschutzvorfällen			
12.1	Prozesse zur Identifikation, Bewertung und Handhabe von Sicherheits- und Datenschutzvorfällen sind eingeführt und geschult.	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	
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	

3.2 Standard-TOM für die Verarbeitungskategorie Data Center Public Cloud

Für die Verarbeitungskategorie „Data Center Public Cloud“ gelten die nachstehenden Standard-TOM der Public Cloud Provider. Der konkret zutreffende Public Cloud Provider wird im Auftragsverarbeitungsvertrag als Unterauftragsverarbeiter genannt.

3.2.1 Amazon Web Services

AWS Data Processing Addendum – Annex 1 Security Standards:

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

3.2.2 Microsoft

Data Protection Addendum – Appendix A Security Measures

https://www.microsoft.com/en-us/licensing/product-licensing/products

3.2.3 Google

Cloud Data Processing Addendum (Partner) – Appendix 2 Security Measures

https://cloud.google.com/terms/data-processing-terms/partner/

4 Definitionen Verarbeitungskategorien

4.1 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.

4.2 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.

4.3 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-Infrastruktur ausschließlich die TOMs des jeweiligen Data Center des Auftraggebers. Der Auftraggeber ist für die TOMs und deren Ausprägung vollumfänglich verantwortlich.

4.4 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.

4.5 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.

4.6 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.

4.7 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 Microsoft 365 Umfeld.

4.8 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.

5 Arvato Systems Gruppe

Die Arvato Systems Gruppe ist unter der E-Mail-Adresse: info@arvato-systems.de zu erreichen und umfasst die unter folgender URL gelisteten Gesellschaften: www.arvato-systems.de/arvato-systems-unternehmensgruppe.