Appendix TOM

Technical and organizational measures of the Arvato Systems Group

Version 4.2

Public

Disclaimer

Contents

1 Introduction

This appendix describes the technical and organizational measures (TOM) of the Arvato Systems Group in accordance with Article 32 of the GDPR.

All processing that Arvato Systems performs on behalf of clients is divided into processing categories. These are defined in Section 4. They are essentially distinguished by the storage location:

- Services with hosting from Arvato Systems' own data centers (Data Center Arvato Systems)
- Services with hosting services on a public cloud environment for which Arvato Systems is responsible (Data Center Public Cloud)
- Services that do not require a data center or are based on hosting services provided by the client (Data Center Customer).

The agreed measures may vary per processing category.

2 Agreement on concrete technical and organizational measures

The technical and organizational measures concretely implemented by the Contractor result from

- the main contract including all appendices such as the service descriptions of the main contract as well as additionally
- the general technical and organizational standard measures in section 3, whereby the applicable processing categories in each case is agreed in the data processing agreement.

In addition to the agreed measures, Arvato Systems offers further security measures or cyber security services that can be additionally ordered by the client.

It should be noted that the security of the client's overall solution results from the coordinated technical and organizational measures of all parties involved in the solution.

3 General technical and organizational standard measures

The following technical and organizational measures are minimum standards for processing at Arvato Systems and apply to assets, systems and processes for which Arvato Systems is the owner or is specified in the contract as "accountable (= accountable for the service or makes related decisions)".

3.1 Standard TOM for processing activities at Arvato Systems

The following standard TOM apply to the following processing categories.

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

For each of these processing categories, the measures ticked in the "general" column apply. For the processing category "Data Center Arvato Systems", additional measures apply which are ticked in the corresponding column.

No.	Measure	general	Data Center Arvato Systems
1. Organization of Data Protection and Information Security			
1.1	Rules and regulations exist for information security and data protection.	x	
1.2	The rules and regulations for information security and data protection are regularly reviewed for compliance and effectiveness.	x	
1.3	The security concepts and measures and their implementation are reviewed regularly.	x	
2. Human Resources Security			
2.1	Employees go through a starter-changer-leaver process, which takes into account security requirements when filling, changing and terminating jobs.	x	
2.2	Employees are committed to observe data protection secrecy.	x	
2.3	Employees are regularly trained on data protection and information security.	x	
2.4	Instructions are established for handling, processing and forwarding of information, the use of mobile devices and storage media as well as the design of working environments (acceptable use policy, clean desk policy).	x	
2.5	Employees are instructed and trained to adequately protect company information, especially in the mobile work environment - from unauthorized third parties viewing the screen by using privacy film and locking of mobile devices when not in use - from unauthorized third parties viewing work documents/printouts through a clean desk policy - from unauthorized third parties taking note of confidential conversations or telephone calls - by keeping mobile devices and equipment appropriately safe - by compliant disposal of paper and data storage devices. Compliance with the instructions can be checked by the employer.	x	
3. Asset Management			
3.1	Processes to maintain an asset inventory and records of processing activities are defined and established.	x	
3.2	Specifications for the classification of data into different protection levels are established.	x	
3.3	Transports of data storage devices containing personal data are subject to a control and documentation process. Data storage devices are transported outside the area of the company in secured, locked transport containers by special courier services or secured with procedures such as encryption.	x	
3.4	Procedure for the disposal of devices, data storage devices and confidential documents is established which include specifications for the deletion of information or destruction by specialized and certified companies in accordance with current standards.	x	
4. Physical and Environmental Security			
4.1	Physical security controls for offices, rooms, and facilities are designed and implemented.	x	
4.2	There is a documented procedure for granting, changing, and withdrawing physical access rights, including the return of access equipment.	x	
4.3	Security areas (areas with higher security requirements) are defined, divided into security zones and documented together with the physical protection measures in a security zone concept.		x

No.	Measure	general	Data Center Arvato Systems
4.4	Secure areas are protected by appropriate access controls and physical barriers depending on the security zone according to the security zone concept. Access to security zones is controlled and approved to allow access to authorized persons only. Access controls that allow visitors to enter security zones are defined.		x
4.5	Access to the Arvato Systems' Data Centers is tracked via a personally assigned means of access with two-factor authentication or comparable protection method.		x
4.6	All visitors to the Arvato Systems' Data Centers are recorded with the date and time of their entry and exit and are escorted by authorized personnel.		x
4.7	Arvato Systems' Data Centers are physically secured, protected with intrusion alarm systems and entrances are monitored with video systems.		x
4.8	Arvato Systems' Data Centers are protected from technical impairments, and elementary environmental hazards - in particular fire, water, failure of supply networks (e.g., UPS, emergency power system, fire extinguisher, fire detection, etc.). Any deviations from normal operation can be quickly detected and remedied.		x
4.9	Arvato Systems' Data Center infrastructure is maintained according to the manufacturer's specifications.		x
4.10	Physical assets and server systems are located in a security zone that meets their protection requirements.	x	
5. System Access Control			
5.1	Within the Identity & Access Management, processes for the allocation, modification and withdrawal of accounts and access rights are documented and in place.	x	
5.2	Request for access creation or modification are documented and approved by the relevant approver.	x	
5.3	Each account is always linked to a specific natural person.	x	
5.4	Accounts and credentials can be blocked immediately.	x	
5.5	Conformity of mobile devices with defined policies is monitored. In case of non-compliance, access is denied.	x	
5.6	Measures are implemented for the protection of user/password authentication.	x	
5.7	Passwords of sufficient complexity and length are used. The structure and handling of passwords shall be in accordance with a documented password policy.	x	
5.8	Default passwords are changed immediately after installation. Initial passwords are individualized.	x	
5.9	Separate accounts/roles and credentials are issued for administrator activities. Administrator accounts are not used for normal office activities.	x	
5.10	Administrator activities with privileged access rights in Arvato Systems' Data Center are carried out via jump servers, virtual desktops in the Data Center and a PAM (Privileged Access Management) system.		x
5.11	By default, devices and sessions are locked automatically after a defined period of inactivity.	x	
5.12	All access to systems (mobile devices, applications, operating systems, BIOS, boot devices, etc.) is protected or blocked.	x	

No.	Measure	general	Data Center Arvato Systems
5.13	Employees use company-provided hardware and software, including standard communications software, for work-related activities. Exception for mobile working: Devices required for the Internet connection and, if necessary, own peripheral devices (e.g., printer, monitor, mouse, keyboard), if these have been purchased as common brand devices from a trustworthy source.	x	
6. Data Access Control			
6.1	Only those access rights are granted that are required to fulfil the respective task (need-to-know and least-privilege principle).	x	
6.2	Granted access rights are reviewed in regular intervals defined by the criticality of the access rights in scope. Active reapproval is required for high critical accounts. Access rights are revoked as soon as they are no longer required	x	
6.3	Role-based access controls are implemented in all systems/applications.	x	
7. Encryption			
7.1	Data on mobile devices is encrypted according to the state of the art and protected against undetected manipulation.	x	
7.2	Data is protected against unauthorized disclosure and manipulation when transported over public networks. (e.g. transport encryption via TLS).	x	
7.3	To support cryptographic measures and techniques, an appropriate cryptographic key management is implemented.	x	
7.4	Implemented cryptographic controls are in line with best practices. Insecure (outdated) techniques are timely replaced.	x	
7.5	The specifications for encrypting the data are agreed between the Client and the Contractor prior to implementation and specified in the service specifications.	x	
8. Pseudonymization			
8.1	The specifications for pseudonymization are agreed between the Client and the Contractor prior to implementation and are specified in the service specifications.	x	
9. Operations			
9.1 Operations - Change Control			
9.1.1	Part of a new or to be changed processing activity is an assessment of the risks of the data subjects and, depending on this, the identification and implementation of technical and organizational security measures.	x	
9.1.2	The IT operating procedures are documented in a comprehensible manner, are regularly checked, and adjusted if necessary.	x	
9.1.3	Changes to information processing systems are subject to a change management process.	x	
9.1.4	Rules for software installation and configuration by users on notebooks are defined, implemented, and monitored.	x	
9.1.5	To decrease the risk of misuse of supporting assets, the authorization and execution of operational procedures are segregated by different roles.	x	
9.2 Operations - Separation Control			
9.2.1	Personal data of clients are processed in such a way that the client can be identified in the processing. Thus, the data of different clients are always physically or logically separated.	x	

No.	Measure	general	Data Center Arvato Systems
9.2.2	Development, test, and production environments are separated.	x	
9.3 Operations - Protection against Malware and Vulnerabilities, Patch Management			
9.3.1	Up-to-date protection against malware and malicious activities is installed and activated on all relevant information systems and mobile devices.	x	
9.3.2	For all systems, new security updates and patches are applied in a timely manner, considering system dependencies, the impact on ongoing operations as well as the damage impact of a vulnerability and the threat exposure.	x	
9.3.3	Software is installed according to specified configuration and hardening standards.	x	
9.3.4	Information is obtained about technical vulnerabilities of information systems in operation. For all systems the exposure to vulnerabilities is evaluated regularly depending on system criticality. Appropriate remedial measures are taken to counteract the exploitation of technical vulnerabilities.	x	
9.3.5	Penetration tests are planned and performed in defined intervals based on the criticality and exposure of the systems in scope.	x	
9.4 Operations - Availability			
9.4.1	The specifications for Client's Data (Back-up and recovery, redundant systems, geo-redundant Data Center, etc.) are agreed between the Client and the Contractor prior to implementation and specified in the service specifications.		x
9.4.2	Backup and recovery procedures are tested regularly, especially after changes to the backup configuration.		x
9.4.3	A process is established to test redundant systems regarding availability requirements.		x
9.4.4	The use of IT resources is monitored and adjusted in line with current and expected capacity requirements.		x
9.5 Operations - Network			
9.5.1	The Arvato Systems network is managed appropriately to protect the information in systems and applications. It is divided into different zones.	x	
9.5.2	External access (remote access) to Arvato Systems' networks and systems is secured and encrypted and requires two-factor authentication.	x	
9.5.3	Only sufficiently secured mobile devices are granted access to the Arvato Systems network.	x	
9.6 Operations - Logging and Monitoring			
9.6.1	Logs recording activities (incl. administrative activities), exceptions, errors, and other relevant events are produced and stored. The level of detail of the logs is determined by the sensitivity of the information and the criticality of the system, and allows to track inputs and changes of personal data.	x	
9.6.2	Network traffic between the network zones is logged and monitored.	x	
9.6.3	Event messages generated on the notebooks for the detection of information security incidents are transmitted to central servers for evaluation.	x	
9.6.4	Log equipment and log data under the accountability of Arvato Systems is protected against unauthorized access, modification, and deletion.	x	
9.6.5	The clocks of critical systems are synchronized with a reliable and agreed time source.	x	

No.	Measure	general	Data Center Arvato Systems
9.6.6	The degree of monitoring of system and network resources is determined in line with a risk assessment.	x	
9.6.7	Roles and responsibilities for protection against cyber threads are defined and implemented (Security Operations Center). Log data is analyzed for security events.	x	
10. Acquisition, Development and Maintenance of IT Systems			
10.1	There are specifications for software development and the acquisition of IT systems and IT services that include the aspects of IT security and data protection by design and by default.	x	
11. Supplier Management			
11.1	Agreements on the exchange of information are concluded and consider the security of information.	x	
11.2	Prior to engaging external subcontractors, an assessment of the risks regarding data protection and information security is carried out in relation to their future tasks. The selection of a suitable subcontractor is based on the results of this assessment.	x	
11.3	Compliance with the data processing agreements is assessed and reviewed regularly.	x	
12. Information Security and Data Protection Incident Management			
12.1	Processes for identifying, assessing, and handling security and data protection incidents are in place and trained.	x	
12.2	Central functions are responsible for coordinating and responding to information security and data protection incidents, performing the assessment, and deciding on the classification of incidents.	x	
13. Business Continuity Management			
13.1	There is a documented business continuity management procedure. Processes and responsibilities are defined to carry out the crisis management and corresponding exercises take place regularly.	x	

3.2 Standard TOM for the processing category Data Center Public Cloud

For the processing category "Data Center Public Cloud", the following standard TOM of the public cloud providers apply. The specific applicable public cloud provider is named in the data processing agreement as a sub-processor.

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

Microsoft Products and Services Data Protection Addendum - Appendix A Security Measures

https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

3.2.3 Google

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

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

4 Definitions processing categories

4.1 Data Center Arvato Systems

In the processing category "Data Center Arvato Systems", the Arvato Systems Group includes all processing and services for its clients that are related to the provision and maintenance of servers, storage, networks, private cloud, or other data center infrastructure located in one of Arvato Systems' data centers.

4.2 Data Center Public Cloud

In the processing category "Data Center Public Cloud", the Arvato Systems Group includes all processing and services for its clients that are connected with the provision and maintenance of servers, storage, networks or other data center infrastructure located in an external public cloud data center commissioned by Arvato Systems. This is done in cooperation with external public cloud infrastructure providers such as Amazon Web Services, Microsoft or Google.

4.3 Data Center Customer

If the Client's data or hardware is located in a data center for which the Client is responsible or which the Client has commissioned, the TOMs of the Client's respective data center shall apply exclusively to the provision of this data center infrastructure. The Client shall be fully responsible for the TOMs and their characteristics.

4.4 Platform Services

The processing category "Platform Services" includes all processing operations in connection with the system administration of IT components, the start-up, configuration, maintenance and operation of basic software components (in a data center and for the IT applications based thereon) such as databases, SAP Basis, SharePoint farms, firewalls and virus scanners or backup and recovery services.

4.5 Application Management & Services

The processing category "Application Management & Services" covers all processing operations in connection with the complete life cycle of IT applications. This includes application development (analysis, design, development and testing) of IT applications on the one hand and application operation (start-up, operation and maintenance) of IT applications by Arvato Systems on the other.

Depending on the assignment, this may also include other services provided by Arvato Systems in connection with the IT application, such as user support, administration of authorizations, creation of evaluations/reports, data analyses or migrations in accordance with the client's specifications.

4.6 Business Process Services

The object of "Business Process Services" is the execution and support of Client’s IT-controlled business processes by Arvato Systems, e.g. newsletter mailing or call center activities. This is made possible by the use of Arvato Systems employees or contracted service providers.

4.7 Workplace Services

The processing category "Workplace Services" includes all processing operations in connection with the provision, administration and support of IT-supported workplaces of the client. This includes the provision and (software) configuration of PCs, notebooks, printers or mobile devices by the Arvato Systems Group as well as the provision of a client service for user requests but also, for example, identity

management or the operation and administration of directory services, file servers or mobile device management solutions. In addition, this processing category also includes mail & collaboration services such as the administration of e-mail, messaging, chat or voice services or telephone systems in cooperation with various technology partners, especially in the Microsoft 365 environment.

4.8 Security Operations Center

Processing operations in the "Security Operations Center" processing category include services that, depending on the assignment, support the client in protecting its networks and systems against the various forms of cyber threats.

Services for protection, detection and reaction are offered in accordance with the Defense in Depth approach. By analyzing network traffic or log data, attacks can be detected (Detection) and responded to in an orderly manner (Reaction). Monitoring of security tools and professional vulnerability management (Protection) increase network security.

These services secure the client's infrastructure in the Arvato Systems data center, in the client's own data center and in the cloud infrastructure, depending on the assignment.

This also includes network security services such as security consulting, vulnerability scanning services or active security monitoring with a security information and event management (SIEM) system, etc.

5 Arvato Systems Group

The Arvato Systems Group can be reached at the email address: info@arvato-systems.de and includes the companies listed at the following URL: www.arvato-systems.com/arvato-systems-group.