1 Pseudonymization and encryption of personal data (Art. 32 (1) lit. a GDPR)

1.1 Pseudonymization

Measures for processing personal data in a way that the personal data cannot be associated with a specific data subject without using additional information, provided that this additional information is kept separately and is subject to technical and organizational measures

1.1.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

Personal data are pseudonymized for processing as far as possible and as requested by the client: By applying pseudonymization to personal data, the risk for the respective person can be reduced.

Roles authorized to manage the pseudonymization, to implement the pseudonymization, and, if necessary, the de-pseudonymization have been defined.

Pseudonymization may take place by encrypting or removing all personal data for certain types of processing. In this way, the personal data or data that could be traced to persons are no longer identifiable for the recipient and can only be associated with the remaining data by means of an identical code, e.g. separation of customer master data and customer sales data. The processing takes place by means of a code instead of the name. The requirements are coordinated between the client and the provider prior to the implementation and specified in detail in the specification sheets.

1.1.2 **Public cloud**

Personal data are pseudonymized for processing as far as possible and as requested by the client. Roles authorized to manage the pseudonymization, to implement the pseudonymization, and, if necessary, the de-pseudonymization have been defined.

1.2 Encryption

Use of procedures and algorithms that transform the content of personal data into an illegible form by means of digital or electronic codes or keys. This can be done by means of symmetric and asymmetric encryption technologies.

1.2.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

For the purpose of the order data processing, the client alone decides which encryption is to be used, and when; for example, this could be data at transport, data at rest, or end to end.

Remote access takes place via a VPN (Virtual Private Network) connection or in encrypted form to the terminal server.

Mobil storage media that contain personal data or company and business documents must always be encrypted.

Various options for symmetric or asymmetric encryption can be implemented and specified in detail in the specification sheet at the request of the controller (e.g. use of SSL certificates for encrypted web communication, SSL VPN for secure connection) to protect their data.

Encryption takes place in line with the state of the art.

1.2.2 **Public cloud**

For the purpose of the order data processing, the client alone decides which encryption is to be used. The keys must be protected against unauthorized access.

Content is not accessed or used unless this is necessary in order to maintain or offer the service offerings or unless this is required in order to comply with the law or with a binding order from a governmental body.

2 Confidentiality (Art. 32 (1) lit. b GDPR)

2.1 Physical access control

Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used

2.1.1 **DC outsourcing / (virtual) private cloud**

The data center rooms protect the clients' infrastructure from unauthorized access and additionally protect the high availability of the building technology for the data center operation.

The premises on which the data centers are located are subject to strict security regulations for the access authorization.

Only authorized persons are granted access to the data centers through different, independent access systems.

The staff record all visitors to the data centers with the date and time of their entrance and departure. Moreover, entrance to the site is granted only for specifically authorized purposes; instructions concerning the security requirements in the area and concerning emergency procedures are given where necessary. The authorization to access the data center also requires a signed personal commitment to the rules of conduct and guidelines within the data center areas.

At some locations, the plant security service patrols the site at varying intervals. Additionally, all building sections of the data center are protected with intrusion detection systems.

Moreover, the internal and external entrances of the data centers are covered by round-the-clock CCTV surveillance.

At different locations, various security zones can be defined in the building, e.g. control room, server areas, data archive or client segments. Generally, access takes place by means of a personally assigned, verifiable access card of the authorized person. Authorization for the individual zones is implemented by means of an authorization process and is granted only to the extent necessary for the business model.

Every external visitor is accompanied by an internal employee during the entire visit in the DC. Service providers are only permitted to enter the DC rooms under supervision.

2.1.2 **Services without direct DC connection**

The following physical security measures apply to all locations or processing not directly related to the DC.

Access controls ensure authorized-only access for employees of the company. Depending on the location, authorized-only access to offices during normal working hours is ensured by means of turnstiles, a second security door, lock systems, cylinder locks, door transponders, authorized employee ID cards (RFID ID card), automated access control systems (card reader) with personalized access cards, access keys for authorized internal employees. The handout of keys is documented in a key book.

Visitors are met by a contact at the entrance and accompanied during the entire stay on the premises.

The plant security service patrols parts of the site at varying intervals, or the building sections are protected with intrusion detection systems. At some locations, the entrance area, the lobby, the elevators, and the access to the offices are covered by indoor and outdoor round-the-clock CCTV surveillance.

2.1.3 **Public cloud**

At some cloud providers, the buildings are supervised and monitored by guards and, in sensitive areas, additionally monitored with CCTV surveillance.

An access authorization concept exists on the basis of a lock system (partially with a proper key management) and an electronic access control system.

Access to individual production areas and the business area is restricted by means of an electronic access control system, e.g. with magnetic cards.

Visitors are only granted access to sensitive areas by prior appointment. In the course of the accreditation, the visitor is provided with a form of identification, e.g. a visitor ID card, which identifies him / her as a visitor and that he / she is required to carry with him during his stay at the location. At some locations, dealings with guests are governed by a policy. Access to the individual production areas is only permitted when accompanied by authorized staff.

2.2 System access control

Measures to prevent unauthorized use of data processing systems

2.2.1 **DC outsourcing / (virtual) private cloud**

All systems and applications require authentication to use the services.

Access to the processing systems takes place with a unique personal user ID and a password. Passwords are assigned in accordance with the password policy. To name just a few: Requirements for the password quality, forced password changes, or blocking of the user account after repeated login attempts with the wrong password in order to avoid risks (to prevent brute force attacks).

The employees go through a starter/changer/leaver process. Here, the responsible managers grant authorization on the basis of the "least privilege" principle to ensure user control.

System administrators and normal users are assigned separate user accounts. For privileged rights, the authorization is regularly verified.

To avoid any risk, the information security policy stipulates that remote access to the network must be subject to the use of two-factor authentication methods (secure ID cards or certificates).

The protection of all networks against access from the outside is regulated by firewalls. By default, it takes place via a security infrastructure chain comprising a proxy, virus scanner, and firewall. At some locations, the special role of the network security officer may be responsible for this area.

It is possible to provide an intrusion prevention system (IPS) for the active prevention of network attacks (remote access, access control lists, special WAN areas, etc.), which, if ordered, can be defined in the specification sheet for the various types of processing and included in the price.

2.2.2 **Services without direct DC connection**

The employees go through a starter/changer/leaver process. Here, the responsible managers grant authorization on the basis of the "least privilege" principle.

Access to the processing systems takes place with a unique personal user ID and a password. Passwords are assigned in accordance with the password policy. To name just a few: Requirements for the password quality, forced password changes, or blocking of the user account after repeated login attempts with the wrong password in order to avoid risks (to prevent brute force attacks).

For privileged rights, the authorization is regularly verified. System administrators and normal users are assigned separate user accounts.

To avoid any risk, the information security policy stipulates that remote access to the network must be subject to the use of two-factor authentication methods (secure ID cards or certificates).

The protection of all networks against access from the outside is regulated by firewalls. By default, it takes place via a security infrastructure chain comprising a proxy, virus scanner, and firewall. At some locations, the special role of the network security officer may be responsible for this area.

2.2.3 **Public cloud**

Regulations exist for the access to IT systems.

These regulations (e.g. the password convention) determine details such as a minimum length and requirements for passwords (e.g. upper and lower case letters, numbers, and special characters, maximum period of validity, trivial password check).

The login and logout actions of the users on the IT systems are logged.

When leaving the workstation, it must be locked or shut down. If this is forgotten, the workstation will automatically lock itself.

Additionally, an access authorization concept exists. As a general rule, all authorizations are withdrawn and must be granted explicitly. The access authorization concept is based on the principle of user roles and profiles. The personalized authorizations are granted by the responsible departments.

Excerpts and summaries of the respective regulations can be made available on request.

2.3 Data access control

Measures to ensure that persons authorized to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified, or removed without authorization in the course of processing or use and after storage

2.3.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

The access control is based on a role-based authorization concept for system access and administration rights graded according to the fields of duty. As a matter of principle, all administrative activities are logged on the systems and can thus be traced. The access rights are granted according to the need-to-know principle. Only the access rights required for the performance of the tasks are granted. The authorized manager is responsible for complying with the need-to-know principle.

When access is set up for a user, the user is merely granted minimum standard authorizations. These may only be expanded by way of defined application routes, subject to the approval of the responsible supervisors/managers in order to comply with due functional separation in the authorization process (double-checking principle).

Remote access takes place via a VPN (Virtual Private Network) connection or in encrypted form to the terminal server.

2.3.2 **Public cloud**

An authorization concept exists for the access to the IT systems.

The objective is to ensure a secure, transparent, and uniform release and authorization strategy on all IT systems. The access takes place according to the "least privilege" concept.

Only authorized storage media shall be used. Employees of the cloud provider are subject to extensive restrictions and approval requirements for the storage of personal data of the client on mobile storage media, processing outside the premises of the cloud provider, or access to these from there.

Access to the individual systems is controlled by means of special network authorizations and a client-based role concept (e.g. administrator, IT, etc.). Access rights are duly documented. Access authorizations are withdrawn/deleted.

The cloud provider informs his staff about all relevant processes and role concepts and describes the consequences of the violation of the respective requirements.

Excerpts and summaries of the respective concepts can be made available on request.

2.4 Transmission control

Measures to ensure that personal data are not read, copied, changed, or removed by unauthorized parties while being transported or saved onto storage devices and to ensure that the planned location of personal data transfer can be checked and determined

2.4.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

To minimize the risk for the data subject, the employees are instructed to use only secure data buses that are defined as mandatory in the privacy policy. The possible data transmission can take place over trustworthy lines and networks that cannot easily be intercepted.

Various options such as the use of SSL certificates for encrypted web communication, SSL VPN for secure connection (secure remote access), electronic signature, logging can be implemented on request and be documented and evaluated in the specification sheets.

For the purpose of the order data processing, the client alone decides which data are to be transmitted and which transmission paths and transmission type are to be used. Additionally, the network segments can be segregated from each other by means of access control lists, and the entire network can be secured by multi-level firewall systems. If a data line that is not trustworthy needs to be used for a transmission,

the transmission can also be encrypted (e.g. via VPN, TLS, etc.).

Data is backed up using removable storage media and VTL libraries, which are subject to automated inventory and stored in a secure area.

To ensure transport control, storage media are only transported or shipped if this has been requested by the client. The client also determines the transport route, e.g. dispatch by registered mail/insured parcel or use of secured/locked transport containers as well as special courier services (encrypted dispatch). This is subject to a control and documentation process.

If storage media need to be destroyed, this is handled by a specialized, certified company according to applicable standards. Until the destruction, the storage media are kept in a secure area and are protected from unauthorized access. The destruction of storage media of the controller and the logging of this destruction always take place according to the order and as instructed.

The information security policy stipulates rules of conduct for the use of mobile storage media (USB stick, CD, DVD, etc.). These rules ensure that personal data or company and business documents are always stored on mobile storage media in encrypted form. Within the scope of the storage media control, this prevents the unauthorized reading, copying, modification, or deletion of storage media.

Rules of conduct exist for the secure destruction/disposal of storage media and confidential documents.

2.4.2 **Public cloud**

Data transmissions take place in the secure network (e.g. with encryption). The electronic transmission of data on public routes or over public networks is always encrypted. In coordination with the recipients, various procedures are used for this purpose.

The use of portable devices (e.g. their connection to a system) is subject to special regulations. Devices no longer used are duly disposed of under consideration of the protection of personal data (e.g. physical destruction). Moreover, various protective mechanisms are employed in order to protect the data (e.g. firewalls, regulations on the procedure to be followed in the event of incidents).

Excerpts and summaries of the respective concepts on the corresponding procedures can be made available on request.

2.5 Separation control

Measures to ensure that data collected for different purposes can be processed separately

2.5.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

The data are separated according to the client's instruction. The various options are defined and evaluated for the various processing types in the specification sheet.

Examples of logical or physical separate at client and/or data level: Functional separation of production / integration / test systems, use of different databases, use of access control software and setup of access rights (including logging), different types of encryption for individual data records, logical separation (e.g. on shared systems), physical separation (e.g. on dedicated systems), etc.

When working remotely, the employee accesses the predefined infrastructure that enables him to process the data according to the defined requirements.

2.5.2 **Public cloud**

Based on the authorization concept, measures (e.g. shares) are implemented on the systems in order to ensure strict separation of data and files from other clients. The access of customers to instances that do not match the access authorizations is effectively prevented.

Test, production, and integration systems are run separately from each other.

3 Integrity (Art. 32 (1) lit. b GDPR)

3.1 Input control

Measures to retroactively check and determine whether and by whom personal data in data processing systems has been entered, changed, or removed

3.1.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

The input control as well as the period for which the resulting data are retained are governed by the client's instructions for his data and on his infrastructure or in his applications.

Optional logging and audit-proof filing of the logs are possible on request and must be defined in the specification sheet.

Administrative access to the systems can be traced by means of standard logging at the operating system level. This serves the detection of unauthorized change or erasure of saved personal data within the scope of the storage control.

The input control is analyzed if necessary within the scope of the instruction through manual or automated log analysis.

3.1.2 **Public cloud**

Where the input, alteration, and deletion of the data takes place on IT systems, the changes to these data are logged with the help of suitable logging and log analysis systems (e.g. access ID, access time, authorization, and activity).

Excerpts and summaries of the respective concepts on the corresponding procedures can be made available on request.

3.2 Organizational and technical protection of authorizations, logging measures, log analyses/audit, etc.

Further information on the protection of authorizations is documented in detail in the chapters "System Access Control" and "Data Access Control". Log analyses must be requested within the framework of the instruction and will be performed in this scope. Any specific details shall be included in the respective specification sheet.

4 Availability and resilience (Art. 32 (1) lit. b GDPR)

4.1 Availability control

Measures to ensure that personal data are protected against accidental loss or destruction

4.1.1 **DC outsourcing / (virtual) private cloud**

All facilities of the data center are physically protected against security threats and environmental dangers.

Different graded security arrangements to ensure availability can be defined and detailed for the business model in the specification sheet.

Some possibilities: Redundant power supply, HA power supply (partially secured by UPS) with static transfer switches (STS), diesel gensets for emergency power supply, HA air-conditioning, fire alarm systems with early fire detection and direct notification of the local firefighters, separate fire zones for each data center, intrusion detection system with door opening control, emergency concepts and plans, redundant network connections and network infrastructure, clustered systems, or redundant hardware (from components to entire servers – geo-redundancy).

These security facilities are regularly reviewed for operational and technical reliability.

Optionally, collaboration with external data centers is possible via sub-contractors; on request, these are available for test operation, redundancy concepts (geo-redundancy) at the application level (by means of clusters, separation of data centers, separate data mirrors, etc.).

Depending on the earmarking of the respective processing, various archiving options are available for a full backup, e.g. regular automatically initiated and monitored backups (usually one full backup per calendar week, daily incremental backups). The normal retention period for these backups is governed by the instruction and is documented in the specification sheet. The backup may take place on a separate backup system that is based in a different fire zone or a different location than the productive system.

Virus protection is used on all workstations of Arvato Systems. The existence of virus protection and the regular update of the virus signature is ensured by using a centrally controlled client anti-virus and firewall solution.

The timely installation of security updates for the utilized operating systems and application programs is required by group policies and ensured by monitoring the patch level.

Topics related to BCM (business continuity management) are described in more detail in the chapter "Incidence Response Management".

4.1.2 **Services without direct DC connection**

The processing of the data by employees takes place via remote/WLAN in the relevant client data center and is thus also subject to the availability of this data center.

All employees have been instructed not to store any work-related data on the laptop, but to use the backup-protected shares set up for this purpose in order to prevent the loss of data.

4.1.3 **Public cloud**

A backup concept exists. These documents describe the measures for backing up personal and mission-critical data.

This includes regular full backups. Moreover, electronic images of the respective systems are created at regular intervals and, if necessary, after implementing new IT systems and after significant changes to the setup of a system.

Depending on the process or relevance, the backups are stored in other buildings or externally. Uninterrupted power supply is being set up.

Apart from this, emergency and business continuity plans exist for the cloud provider's facilities.

Excerpts and summaries of the respective concepts on the corresponding procedures can be made available on request.

4.2 Order control

Measures to ensure that personal data processed in the order can only be processed according to the client's instructions

4.2.1 **DC outsourcing / (virtual) private cloud / services without direct DC connection**

The data will only be processed according to the client's instructions. These instructions must at least be given in text formissued only by authorized persons of the client to authorized persons of the provider.

All employees are under the obligation to maintain confidentiality and to comply with special obligations such as the privacy of telecommunications and social privacy. Inspections are performed for the purpose of conducting sample audits.

Data center inspections or audits are possible in the relevant data centers according to the principle of proportionality and after due written notification of the responsible unit. To ensure the protection of the personal data of different controllers, the organization and performance of an audit are subject to the audit policy.

4.2.2 **Public cloud**

The provider has appointed an internal data protection officer. By means of its data protection organization, it ensures his due and effective involvement in relevant operational processes.

Employees are instructed about their roles and responsibilities, e.g. by way of preparatory training sessions. The client has appointed one or several officers to control and monitor compliance with data security requirements.

Documents are kept and reviewed concerning the data protection and data security, responsibilities, and relevant procedures.

The Group Audit department (IT and administrative audits) regularly conducts comprehensive audits within the affiliated companies (pursuant to the definition of Sections 15 ff of the German Stock Corporation Act (AktG)). The Compliance Management department regularly conducts comprehensive audits within the affiliated companies (pursuant to the definition of Section 15 ff of the German Stock Corporation Act (AktG)).

Suitable contracts are concluded with external service providers. The contractual performance is tracked and checked by means of suitable controls.

5 Process for regular testing, assessment, and evaluation (Art. 32 (1) lit. d GDPR; Art. 25 (1) GDPR)

5.1 Data protection management in the Arvato Systems Group

For all legal units of Arvato Systems at which the core business comprises the processing of personal data or special categories personal data pursuant to Art. 9 GDPR or personal data relating to criminal convictions and offenses pursuant to Art. 10 GDPR, an external data protection officer has been appointed. A team of qualified data protection officers who serve as data protection coordinators in the individual legal units can be contacted by e-mail (Datenschutz@arvato-systems.de).

Arvato Systems defines the cornerstones of data protection in the group privacy policy and in more detail in the internal privacy policy of Arvato Systems.

The data protection officer and the IT Audits unit regularly conduct audits to check, assess, and evaluate the effectiveness of the aforementioned measures. Subject to the principle of proportionality, an audit may be conducted by the client after due prior notification for control purposes.

Arvato Systems has the following certifications that substantiate its security-relevant processing: ISO / IEC 27001.

At Arvato Systems, an ISAE report can be obtained to furnish evidence of the due processing and compliance with information security.

The security concept of Arvato System is documented in the group information security policy.

To increase the level of protection when processing personal data for the data subject, the internal privacy policy of Arvato Systems with its approved rules of conduct for all employees shall be complied with. Moreover, the risk is mitigated by means of effective patch management, pen tests, log analyses, focus on web security (e.g. OWASP) and a SOC center. A risk-based approach is preferred for the technical and organizational measures.

The assurance of a procedure for the regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures and of the security of the processing takes place via the following PDCA cycle: Plan (development of a security concept), Do (introduce TOM), Check (monitor the effectiveness / completeness), and Act (continuous improvement).

The transmission of personal data to a third country takes place by coordination between the client and the provider under consideration of standard data protection clauses.

In his own sphere of responsibility, the provider guarantees data protection management at a comparable level as at Arvato Systems.

5.2 Incident response management in the Arvato Systems Group

Measures to quickly restore the availability of personal data and access to these after a physical or technical incident

Within the scope of the established BCM (business continuity management), procedures have been documented to ensure business operations in the event of an emergency or major malfunction and to restore all services to be provided for the client. Recovery drills are regularly conducted.

Measures to ensure the resilience of the systems and services have been arranged in such a way that even processing load peaks or continually high loads can be handled. Subjects related to the storage, access, and line capacities as well as on backup and redundancy concepts have been included in detail in the availability control.

5.3 Data protection by design and by default (Art. 25 (2) GDPR) at Arvato Systems Group

During the product development, the implementation of data protection is realized taking into consideration the internal white paper entitled "Data Protection in Product Development" and a checklist to consider data protection through technical design and data protection-friendly default settings.

Use of the white paper is mandatory in the privacy policy of Arvato Systems.