Appendix TOM

Technical and organizational measures of the

Arvato Systems Group

Assignment of Processing Categories

Gütersloh, May 03, 2019

Table of Contents

1 Introduction

According to Art. 32 DSGVO, persons responsible for data processing are obliged to take technical and organizational protective measures to ensure the security of the processing of personal data.

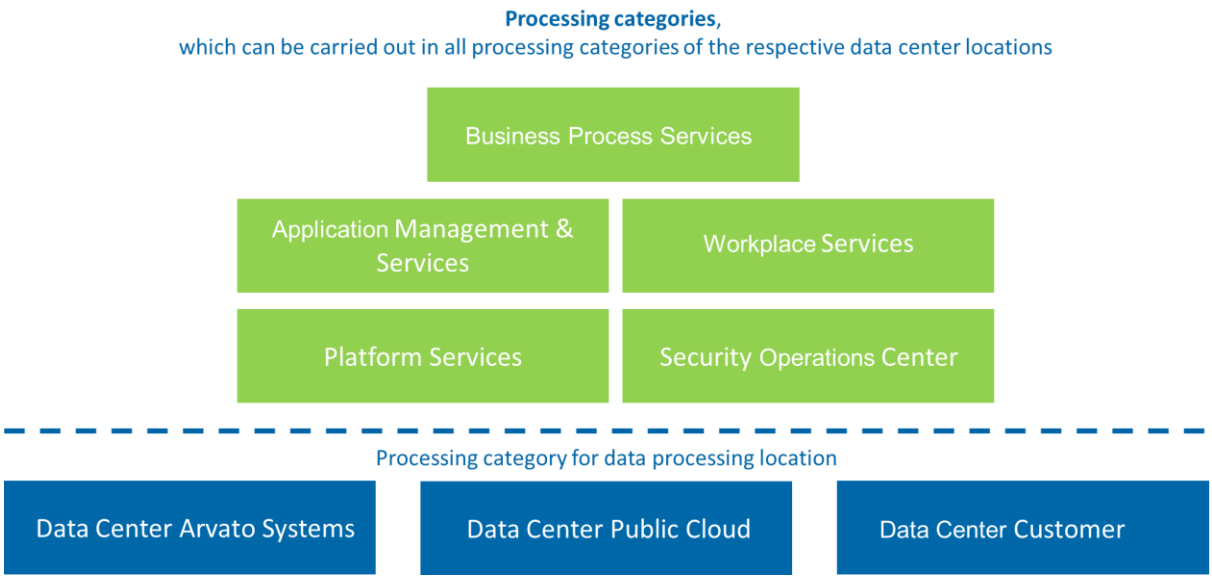
The protective measures must be chosen in such a way that, taken together, they ensure an adequate level of protection.

In the case of processing of personal data by products (finished IPs), an adjustment and/or instruction by the client is only to be implemented within the scope of the product possibilities.

The Arvato Systems Group* has subdivided all processing that it carries out for clients into processing categories. The following text contains short definitions for all processing categories, which document Arvato Systems' understanding of the content of the respective processing category. In addition, for each processing category that is selected in the contract for order data processing for its business model, the client is enabled to assign the relevant technical and organizational measures for this processing category.

This overview explains the protective measures taken by Arvato Systems with regard to the processing of personal data for each processing category.

Arvato Systems has defined three processing categories with data center reference for the client in order to simplify the assignment of the main data processing location. This enables an immediate statement to be made as to whether the main processing is being carried out in one of Arvato Systems' data centers, in a data center of a public cloud service provider (with whom Arvato Systems has concluded a contract) or in the customer data center (where the customer is solely responsible for implementing the technical and organizational measures).



2 Technical and Organizational Measures (TOM) of the Arvato Systems Group* for the Processing Categories Platform Services, Application Management & Services, Business Process Services, Workplace Services and Security Operations Center

2.1 Definition

The following technical and organizational measures (TOM) apply only to the following processing categories and are based on the TOMs of the Data Center defined for the processing in question:

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

2.2.1 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

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 affected person can be reduced.

Roles authorized to manage the pseudonymization, to implement the pseudonymization, and, if necessary, the depseudonymization 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 client master data and client 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.

2.2.2 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.

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.

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

2.3.1 Physical access control

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

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.

2.3.2 System access control

Measures to prevent unauthorized use of data processing systems

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.

2.3.3 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

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.

2.3.4 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.

To minimize the risk for the data subject, the employees are instructed about internal guidelines to use only secure data buses. The possible data transmission can take place over trust-worthy 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 trust-worthy needs to be used for a transmission, the trans-mission 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.

2.3.5 Separation control

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

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.

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

2.4.1 Input control

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

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.

2.4.2 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.

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

2.5.1 Availability control

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

A processing of the data by employees outside the data centers takes place via remote / WLAN in the relevant client data center and is therefore 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.

2.5.2 Order control

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

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.

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

2.6.1 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 da-ta protection officer has been appointed, insofar as this is prescribed by law. 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 IT Audits and the data protection officer (if appointed) 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.

As proof for a security-relevant processing, Arvato Systems can prove certificates. You can find the certificates under the following link: https://www.arvato-systems.com/certifications.

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).

2.6.2 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.

2.6.3 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.

3 Processing category: Data Center Arvato Systems

Data Center Arvato Systems

3.1 Definition 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 connected with the provision and maintenance of servers, storage, networks, private clouds, or other data center infrastructure located in one of Arvato Systems' data centers.

This processing category is used to enable the client to classify his data flow spatially.

Arvato Systems has standardized the following technical and organizational measures for all of its data centers.

3.2 Technical and organizational measures for the Data Center of the Arvato Systems Group

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

3.2.1.1 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

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 depseudonymization 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 client master data and client 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.

3.2.1.2 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.

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.

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

3.2.2.1 Physical access control

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

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. Moreo-ver, 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 au-thorization 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, verifi-able access card of the authorized person. Authoriza-tion 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.

3.2.2.2 System access control

Measures to prevent unauthorized use of data processing systems

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 au-thorization is regularly verified.

To avoid any risk, the information security policy stip-ulates that remote access to the network must be sub-ject 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 sys-tem (IPS) for the active prevention of network attacks (remote access, access control lists, special WAN are-as, etc.), which, if ordered, can be defined in the specification sheet for the various types of processing and included in the price.

3.2.2.3 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

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.

3.2.2.4 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.

To minimize the risk for the data subject, the employees are instructed about internal guidelines to use only secure data buses. The possible data transmission can take place over trust-worthy 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 trust-worthy needs to be used for a transmission, the trans-mission 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.

3.2.2.5 Separation control

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

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 produc-tion / 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.

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

3.2.3.1 Input control

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

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 auto-mated log analysis.

3.2.3.2 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.

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

3.2.4.1 Availability control

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

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, in-trusion detection system with door opening control, emergency concepts and plans, redundant network connections and network infrastructure, clustered sys-tems, or redundant hardware (from components to en-tire servers – geo-redundancy).

These security facilities are regularly reviewed for op-erational 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 mir-rors, 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 re-tention period for these backups is governed by the instruction and is documented in the specification sheet. The backup may take place on a separate back-up system that is based in a different fire zone or a dif-ferent 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 us-ing 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 manage-ment) are described in more detail in the chapter "Incidence Response Management".

3.2.4.2 Order control

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

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.

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

3.2.5.1 Data protection management in the Arvato Systems Group

For all legal units of Arvato Systems at which the core business comprises the processing of person-al data or special categories personal data pursuant to Art. 9 GDPR or personal data relating to crimi-nal convictions and offenses pursuant to Art. 10 GDPR, an external da-ta protection officer has been appointed, insofar as this is prescribed by law. 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 IT Audits and the data protection officer (if appointed) 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 pur-poses.

As proof for a security-relevant processing, Arvato Systems can prove certificates. You can find the certificates under the following link: https://www.arvato-systems.com/certifications.

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 com-plied 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 (moni-tor the effectiveness / completeness), and Act (continuous improvement).

3.2.5.2 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 stor-age, access, and line capacities as well as on backup and redundancy concepts have been included in detail in the availability control.

3.2.5.3 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.

4 Processing category: Data Center Public Cloud

Data Center Public Cloud

4.1 Definition 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.

This processing category is used to enable the client to classify his data flow spatially.

4.2 Technical and organizational measures for the Data Center Public Cloud provider

In this chapter you will find links to the technical and organizational measures (hereinafter TOM) of the major public cloud providers which may apply to your business model. Hereby the client is able to inform himself directly about the current TOM, which are listed in the contract for order processing and are the basis of the respective business model.

4.2.1 Amazon Web Services

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

4.2.2 Microsoft

Overview:

https://www.microsoft.com/en-us/trustcenter/privacy/privacy-overview#section3

Document:

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

4.2.3 Google

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

4.2.4 Oracle

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

4.2.5 SAP

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

5 Processing category: Data Center Customer

5.1 Definition Data Center Customer

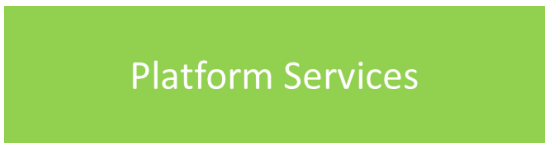
If the Client's data or hardware is located in a Data Center for which the Client is responsible or which has been commissioned, the TOMs of the Client's respective Data Center shall apply exclusively for the provision of this Data Center infrastructure. The client is fully responsible for the TOMs and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

This processing category is used to enable the client to classify his data flow spatially.

5.2 Technical and organizational measures for the Data Center Customer

The customer defines his TOMs and is fully responsible for their development.

6 Processing category: Platform Services



6.1 Definition 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.

6.2 Technical and organizational measures for the Platform Services

The generally applicable technical and organizational measures of the Arvato Systems Group* (see Chapter 2) and the technical and organizational measures of the relevant data centers (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer) apply to this processing category.

7 Processing category: Application Management & Services

7.1 Definition Application Management & Services

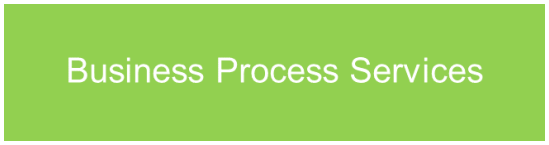
The processing category "Application Management & Services" covers all processing operations in connection with the complete life cycle of IT applications. This includes application development (analysis, conception, development and testing) of IT applications on the one hand and application operation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

Depending on the assignment, this may also include other Arvato Systems support and service provision 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.

7.2 Technical and organizational measures for the Application Management & Services

The generally applicable technical and organizational measures of the Arvato Systems Group* (see Chapter 2) and the technical and organizational measures of the relevant data centers (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer) apply to this processing category.

8 Processing category: Business Process Services



8.1 Definition Business Process Services

The object of "Business Process Services" is the implementation or support of the client's IT-controlled business processes by Arvato Systems, such as newsletter mailing or call center activities. This is made possible by the use of Arvato Systems employees or contracted service providers.

8.2 Technical and organizational measures for the Business Process Services

The generally applicable technical and organizational measures of the Arvato Systems Group* (see Chapter 2) and the technical and organizational measures of the relevant data centers (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer) apply to this processing category.

9 Processing category: Workplace Services

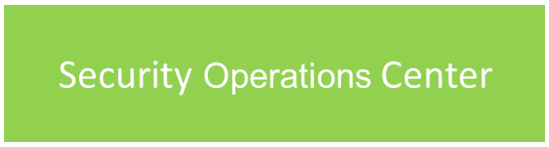
9.1 Definition Workplace Services

The processing category "Workplace Services" includes all processing operations in connection with the provision, administration and support of IT-supported workstations 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. 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 Office 365 environment.

9.2 Technical and organizational measures for the Workplace Services

The generally applicable technical and organizational measures of the Arvato Systems Group* (see Chapter 2) and the technical and organizational measures of the relevant data centers (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer) apply to this processing category.

10 Processing category: Security Operations Center



10.1 Definition Security Operations Center

“Security Operations Center" processing includes services that, depending on the assignment, support the client in protecting his 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 the network traffic or log data, attacks are detected (Detection), which can be responded to in an orderly manner (Reaction). Monitoring of security tools and professional vulnerability management (protection) increase network security.

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

This also includes network security services such as security consulting, vulnerability scan services or active security monitoring with Security Information and Event Management (SIEM), etc.

10.2 Technical and organizational measures for the Security Operations Center

The generally applicable technical and organizational measures of the Arvato Systems Group* (see Chapter 2) and the technical and organizational measures of the relevant data centers (Data Center Arvato Systems / Data Center Public Cloud / Data Center Customer) apply to this processing category.

11 Arvato Systems Group

*The Arvato Systems Group can be reached at the e-mail address: info@arvato-systems.de and includes the following companies:

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