Agreement on Order Processing

This Agreement on Order Processing was published on **01.10.2018** . It entered into force on **01.11.2018**. Version 4.0 was released on **01.01.2020** and enters into force on **15.02.2020**.

Previous versions can be requested at datenschutz@arvato-systems.de

Contractual parties

This Agreement exists between Arvato Systems GmbH, an der Autobahn 200, 33333 Gütersloh and farmpilot customer, which registered via http://portal.farmpilot.de/FarmpilotGUI/#/registration (or a successor page determined by Arvato Systems.

1 Preliminary remarks

The farmpilot customer (hereinafter: **"Customer"**) hereby commissions Arvato Systems (hereinafter: "**Contractor")** with the processing of personal data, which the Customer uses within the farmpilot system.

This Agreement on Order Processing (hereinafter **OP Agreement**") specifies the data protection law obligations of the contractual parties, taking the requirements according to Art. 28 of the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC of 24 May 2016 (hereinafter **GDPR**"). It applies to all activities in which persons deployed by the Contractor process personal data of the Customer.

2 Definition of terms

The terms used in this OP Agreement, such as "personal data", "processing", "controller", "processor" or "data subject" correspond to the definition of terms of the GDPR if no other definitions are included in this OP Agreement. The "data of the Customer" refers exclusively to those personal data which were either transferred to the Contractor by the Customer or were collected exclusively by the Contractor for the Customer on the latter's behalf.

3 Object and duration of processing; nature, purpose and means of processing; nature of personal data and categories of data subjects

3.1 Object and duration

The Contractor shall provide the Customer with farmpilot, a software system which allows the Customer to prepare and monitor logistical orders in agriculture and in the transport sector and to evaluate these orders after they have been processed. This may lead to the storage, transmission, evaluation and modification of personal data in the farmpilot system.

In using farmpilot, the Customer shall commission the Contractor to store the personal data that the Customer enters in the farmpilot system and to display and evaluate this data through the functions that farmpilot offers.

Other details arise from the functional description at www.farmpilot.de (or a successor page determined by Arvato System) and from the General Terms and Conditions of Business for the use of farmpilot retrievable at http://portal.farmpilot.de/FarmpilotGUI/resources/public/doc/agb_de.pdf (or a successor page determined by Arvato).

3.2 Nature of processing

The Contractor shall provide the Customer with the farmpilot standard service with existing standard functionalities. In doing so, he shall use the farmpilot IT infrastructure, the farmpilot app and farmpilot web portal.

The Customer shall enter its own as well as the data of its customer if applicable via farmpilot. This data shall be stored and retrieved in partly processed form. Address data, geo data and additional plot-related information shall be entered in the system by the Customer themselves.

Process-related data, position data and machine data as well as working times of the Customer's staff and/or subcontractors shall be generated during order processing and transmitted to the system through mobile communications.

3.3 Purpose of processing

The Customer handles and administers its operational tasks (e.g. order planning, worktime recording, evaluation of its orders, fleet control) with the assistance of farmpilot. The Customer themselves shall determine what operational tasks it has to handle.

3.4 Means of processing

The means of processing shall be the use of farmpilot functionalities. Examples:

- order processing occurs with the assistance of the farmpilot app
- order planning and fleet control is carried out with the help of the farmpilot web portal
- the data recorded and generated during the work process is stored on the farmpilot infrastructure

3.5 Nature of personal data

- The Customer's address data and that of its customers
- Geo data of plots of land belonging to the Customer or the Customer's customers.
- Plot-related data, such as the name of the plot, the size of the plot, cultivation plans, etc.
- Data concerning the type of jobs to be performed (information about measures)
- Process-related data concerning the job to be performed (data from schedules of measures, photos for documentation)
- Position data of terminals over the course of time
- Machine data generated by various sensors of the working equipment used
- Working times of persons (e.g. of the Customer's staff or subcontractors) as well as supplementary information about these persons (e.g. personnel number, name, service group, telephone number)

3.6 Categories of data subjects

The categories of data subjects depend on the data with which the Customer fills the farmpilot system. Depending on the use of farmpilot by the Customer, this data, for example, may be:

- customer staff
- independent subcontractors
- the employees of independent subcontractors if applicable

4 The Contractor's obligation to follow instructions

4.1 The Contractor may only process the data of the Customer within the framework of this Agreement and the instructions of the Customer - also in relation to the transmission of personal data to a third country or an international organisation in the meaning of Art. 4 (1) no. 26 GDPR (e.g. UN) unless it is legally bound to such processing. In this case, the Contractor

shall inform the Customer of these legal requirements in writing or by e-mail (text form), provided the law involved does not prohibit such notification on account of an important public interest.

4.2 "Instructions" shall be the documented directions of the Customer oriented to the particular processing of the data of the Customer by the Contractor. At first, the instructions shall be set out in this OP Agreement and may later be altered, supplemented or replaced by an instruction from the Customer (individual instruction). Activities of the Contractor on account of instructions that go beyond the contractually-agreed scope of services must be remunerated additionally by the Customer according to expense. The Contractor's usual daily and hourly rates shall apply to services that the Contractor notifies to the Customer on request.

4.3 In general, the instructions of the Contractor must be issued in writing; in exceptional cases, oral instructions required must be confirmed by the Customer immediately in writing. Persons entitled to issue instructions on the part of the Customer and persons entitled to receive them on the part of the Contractor shall be communicated to the other party.

4.4 There shall be no substantive legal due diligence obligation on the part of the Contractor regarding instructions issued by the Customer. However, if the Contractor is of the view that an instruction of the Customer breaches the GDPR or other data protection regulations of the Union or member countries, it shall inform the Customer immediately. The Contractor has the right to suspend the execution of the agreed activity in this respect until the Customer has decided on the further procedure and informed the Contractor in writing. The Customer shall bear any additional expense of the Contractor arising as a result of this. The Customer shall bear the sole responsibility for the decision taken by it. Should the Customer adhere to the instruction issued and should its implementation in the view of the Contractor still require unlawful action by it, the Contractor shall be entitled, (i) to make the corresponding processing dependent on the provision of a security by the Customer (e.g. surety), or (ii) obtain a decision of the responsible regulatory authority, or (iii) not to carry out the processing.

4.5 Should redress be sought against the Contractor or its subcontractors by a third party on account of the implementation of an instruction of the Customer (including those stipulated in the main agreement) or on account of a decision pursuant to subsection 4.4 above with the claim that the third party suffered a tangible or intangible loss on account of a breach of the GDPR, or a regulatory authority as a result of this levies or threatens a fine against the Contractor or its subcontractors, the Customer shall indemnify the party against whom redress is sought in full from such redress or fine. The claim to indemnity in this respect shall also include the appropriate costs of legal defence. This shall apply correspondingly if the redress sought is attributable to breach of the contractual or legal obligations by the Customer.

5 Obligations of the Contractor

5.1 The Contractor shall take technical and organisational measures in its area of responsibility for the appropriate protection of the data of the Customer, which permanently secures the confidentiality, integrity, availability and resilience of the systems and services in connection with this order processing and have the capacity to quickly restore the availability of the personal data and access to them in the event of a physical or technical incident. The technical and organisational measures taken by the Contractors shall be recorded in **Annex 1** (hereinafter "**TOMs**").

5.2 The Client has knowledge of these TOMs. The Client bears sole responsibility for ensuring that they provide a level of security appropriate to the risks applicable to the Personal Data to be processed.

5.3 He agrees to indemnify, defend, and hold harmless the Contractor from and against any and all third party claims resulting from or related to the fact that these TOMs are not sufficient to ensure an appropriate level of security.

5.4 The Contractor shall reserve the right to amend the **TOMs** taken unless the protection level specified in **Annex 1** is thereby undercut.

5.5 The Contractor has established a procedure for regular review of the effectiveness of the **TOMs** to guarantee the security of the processing.

5.6 The Contractor shall guarantee that the employees occupied with the processing of the data of the Customer and other persons employed for the Contractor only process this data pursuant to the instructions of the Customer unless they are legally obliged to such processing. The Contractor shall in addition guarantee that the persons deployed by it for processing of the data of the Customer are committed to confidentiality or subject to an appropriate statutory confidentiality obligation. This obligation shall also continue after termination of the order.

5.7 The Contractor shall notify the Customer immediately if it becomes aware of breaches of the data of the Customer. The Contractor can in this case ad interim and at its own discretion take the appropriate measures on its own responsibility to protect the data of the Customer and to reduce the potential detrimental consequences. The Contractor shall inform the Customer of any measures taken by it as soon as possible.

5.8 The data protection team of the Contractor shall be available to the Customer for data protection queries in the context of this Agreement at dataprotection@arvato-systems.de or at tel. +49 5241 80-70785.

5.9 The Contractor shall be obliged to maintain a record of processing pursuant to Art. 30 II GDPR. The Contractor shall be authorised to provide the records relating to this OP Agreement to a regulatory authority or a third party on its request. The Customer can request this record from the Contractor if a regulatory authority demands it from the Customer or the Customer carries out audits or certifications.

5.10 The Contractor shall support the Customer, taking the type of processing into account and the information available to it in observing the obligations of the Customer regulated in Articles 32 to 36 GDPR.

5.11 The Contractor can demand appropriate remuneration and reimbursement of expenses for the support of the above subsections 5.7 and 5.8.

5.12 Should the data of the Customer be endangered at the Contractor through attachment or seizure, by insolvency or settlement proceedings or other incidents or measures of third parties, the Contractor must inform the Customer immediately of this unless the law involved prohibits such notification on account of an important public interest. The Contractor shall inform the third party immediately that solely the Customer holds the sovereignty and "title to the documents."

6 Obligations of the Customer

6.1 The Customer is the sole master of the data and accordingly the controller in the meaning of Art. 4 no. 7 GDPR. It bears the undivided responsibility within the context of this OP Agreement for the observance of the statutory provisions of the data protection laws, especially for the lawfulness of forwarding the data to the Contractor and for the lawfulness of the data processing. The Customer shall be responsible for meeting the obligations regulated in articles 32 to 36 GDPR.

6.2 The Customer must immediately and fully inform the Contractor if the Customer discovers any errors or irregularities in relation to data protection law provisions when examining the results of the job.

6.3 After conclusion of the Agreement, the Customer shall give the Contractor the name of its contact for any data protection questions that arise. The Customer shall inform the Contractor in writing immediately of any change in the contact in writing.

6.4 The Customer shall provide the Contractor with all information that the Contractor requires for maintaining the records according to Art. 30 (2) GDPR.

6.5 The Customer shall be responsible for evaluating and assessing the effectiveness of the TOMs taken to guarantee the security of the processing.

6.6 In the event of redress being sought against the Contractor by a data subject or body mentioned in Art. 80 GDPR with regard to any claims according to Art. 79 or 82 GDPR, the Customer shall undertake to support the Contractor in mounting a defence against the claims. The Contractor shall in this regard be entitled to disclose details of the OP Agreement, the data processing and instructions of the Customer for the purpose of mounting a defence against these claims or for exculpation according to Art. 82 (3) vis-a-vis third parties.

6.7 The following shall apply if the Customer has to remunerate services or reimburse expenses on account of the OP Agreement: (i) with regard to personnel expenses, the normal daily rates offered by the Contractor shall apply (ii) with regard to other expenses, especially the services of third parties, an appropriate handling fee shall be added.

7 Observance of data subject rights

7.1 With regard to this OP Agreement, the Customer shall be responsible for the observance of the data subject rights provided for according to Chapter III of the GDPR. The Contractor shall support the Customer within the framework of its possibilities with suitable technical and organisational measures in the fulfilment of its obligations in this regard. The Contractor may demand appropriate remuneration for this support and the reimbursement of expenses.

7.2 If a data subject contacts the Contractor with the assertion of data subject rights regulated in the GDPR, the Contractor shall refer the data subject to the Customer if assignment of the data subject question to the Customer is possible according to the information of the data subject.

8 Other order processors

8.1 The Contractor shall be entitled to deploy subcontractors as other order processors.

8.2 The Contractor shall configure the contractual arrangements with the subcontractor to ensure that the same data protection obligations are imposed on the subcontractor vis-a-vis the Contractor as have been determined in this OP Agreement in relation to the Contractor, provided no divergent obligations in favour of a subcontractor have been agreed in this OP Agreement. The above obligation shall in particular apply with regard to the requirements for confidentiality, data protection and data security with regard to personal data.

8.3 A list of the subcontractors of the Contractor is available at https://portal.farmpilot.de/FarmpilotGUI/resources/public/doc/sub_contractors_en.pdf. The URL may be updated by the Contractor from time to time.

8.4 The Contractor shall update the website at least 14 calendar days before new subcontractors are authorised to access personal data. The Customer shall be obliged to check the website for changes (if applicable by suitable technical measures, e.g. automated per google alert).

8.5 If the Customer does not agree to a new subcontractor, it shall be entitled to cancel the Agreement on use of farmpilot within four weeks of publication of the new contractor in text form.

8.6 The cancellation must be addressed to: team@farmpilot.de

8.7 Should the subcontractor fail to meet its data protection obligations, the Contractor shall be liable vis-a-vis the Customer for the observance of the obligations of this subcontractor as for its own fault.

9 Verifications of the Contractor, inspections

9.1 Should necessary data protection law inspections or examinations be required by the Customer or an independent external auditor, whose name shall be communicated in good time to the Contractor (e.g. if the Customer has well-founded doubt regarding a self-audit submitted by the Contractor), these shall be carried out subject to observance of the provisions of the "Guideline for external audits" of the Contractor in the place of business. The Contractor may make these inspections or examinations dependent on the signature of an appropriate confidentiality declaration regarding the data of other customers and the technical and organisational measures established. Should the auditor commissioned by the Customer be a competitor of the Contractor or its subcontractor, the Contractor can refuse an audit by the auditor.

9.2 The Customer shall provide the Contractor with a copy of the complete audit report in digital form. The Contractor may in particular also transfer the audit report to its subcontractors.

9.3 The Contractor may demand remuneration pursuant to the regulations of "Obligations of the Customer" of this Agreement for support in conducting the inspection or examination.

9.4 The right of the Customer to inspection or examination pursuant to the above subsection 9.2 shall be limited to one day per calendar year; divergences must be agreed with the Contractor in text form.

10 Return and deletion of data at the end of the Agreement

10.1 Deletion of personal data If the agreement concerning the use of farmpilot is ended (e.g. by giving notice of termination), the Contractor shall block the customer account at the time when the agreement ends.

10.2 Stored data shall be kept for three months as from the time when the agreement ends. After that the Contractor shall automatically delete the data without further notice.

10.3 Surrender of data The Customer shall be entitled to demand the surrender of its data within this three-month period as long as this is technically possible. Furthermore, the Customer may demand its early deletion. This request must be made in writing. The costs and expenses arising for the Contractor from the deletion or surrender must be borne by the Customer. The currently valid hourly rates of the Contractor shall apply to expenses.

10.4 The obligation to surrender or deletion pursuant to this subsection 10 shall not apply if the Contractor is legally or otherwise obliged to preservation or storage of this data.

11 Control rights of regulatory authorities or other sovereign regulatory authorities of the Customer; cooperation with regulatory authorities; legal disputes

11.1 Should a data protection regulatory authority or another sovereign regulatory authority of the Customer carry out an inspection at the Contractor, the subsections 9.2 and 9.4 sentence 1 of the OP Agreement shall apply correspondingly. Signature of the confidentiality obligation shall not be required in this case.

11.2 The contractual parties shall immediately inform each other of all official enquiries/orders and proceedings, all measures of one of the bodies mentioned in Art. 80 GDPR (such as complaints, warnings assertion of claims) and all imminent or current court proceedings whose subject is the cooperation regulated in this OP Agreement, cooperate closely in connection with these enquiries, orders, measures or proceedings and mutually provide all documents and information required. Each party shall be entitled in this regard to disclose all information and documents relating to this OP Agreement, including details of the data processing, vis-a-vis the regulatory authority or other third party responsible for it if this is necessary from the point of view of the party.

12 Other provisions

12.1 This Agreement shall be an integral part of the General Terms and Conditions of Business for the use of farmpilot, retrievable at http://portal.farmpilot.de/FarmpilotGUI/resources/public/doc/agb_de.pdf (or a successor page determined by Arvato Systems).

12.2 Liability Should the Contractor inflict loss on the Customer through the processing of personal data in breach of the agreement or instructions, the General Terms and Conditions of Business of the Contractor shall apply to the use of farmpilot.

12.3 The provisions of this OP Agreement shall take precedence in the event of a contradiction between the General Terms and Conditions of Business for the use of farmpilot. If no contradictory arrangements are arrived at in this OP Agreement, the General Terms and Conditions of Business shall apply to the use of farmpilot.

12.4 Otherwise, the Miscellaneous Terms of the General Terms and Conditions of Business shall apply to the use of farmpilot subsection 7.8.

13 Annex

Annex 1 Description of the technical and organisational measures pursuant to Art. 32 GDPR

Annex 2 Change history of this order processing agreement

Annex 1

Description of the technical and organisational measures pursuant to Art. 32 GDPR

arvato BERTELSMANN

1 Pseudonymisation and encryption of personal data (Art. 32 [1 a] GDPR)

1.1 Pseudonymisation

Measures to process personal data in a manner to ensure that the personal data can no longer be assigned to a specific data subject without reference to additional information if this additional information is separately preserved and is subject to technical and organisational measures.

1.1.1 **CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection**

Personal data is pseudonymised for processing if possible and ordered by the Customer: The use of pseudonymisation for personal data can reduce the risk for the data subject.

The roles entitled to administration of pseudonymisation procedures, implementation of pseudonymisation and if applicable, depseudonymisation are defined.

Pseudonymisation can occur through encryption or removal of all personal data for particular processing. For this purpose, personal data and data that can be related to a person is rendered unrecognisable for the recipient and can only be connected with the remaining data through an identical identification number, e.g. separation of customer master data and customer sales data. Processing occurs via an identification number instead of via the name. The guidelines shall be discussed and agreed between the Customer and Contractor before implementation and laid out in detail in the specifications.

1.1.2 **Public cloud**

Personal data is pseudonymised for processing if possible and ordered by the Customer. The roles entitled to administration of pseudonymisation procedures, implementation of pseudonymisation and if applicable, depseudonymisation are defined.

1.2 Encryption

Deployment of procedures and algorithms that by means of digital or electronic codes or keys render the content of personal data illegible. Symmetrical and asymmetrical encryption techniques may be used

1.2.1 **CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection**

The Customer alone decides when and which encryption can be used in the interests of the order processing, this could for example be: data at transport – data at rest – end-to-end.

Remote access occurs via a VPN (virtual private network) connection or encrypted to the terminal server.

Mobile data-carriers which contain personal data or operating and business documents always have to be encrypted.

Different options for symmetrical or asymmetrical encryption can be implemented on the request of the responsible party for the protection of its personal data and laid out in detail in the specifications (e.g. use of SSL certificates for encrypted web communication, SSL virtual private network for a secure connection).

The encryptions correspond to the state of the art.

1.2.2 **Public cloud**

The Customer alone decides when and which encryption can be used in the interests of the order processing. The keys must be protected against authorised access.

Access or use of the contents does not occur unless it is necessary in order to maintain or offer the service products, or is required to observe the laws or comply with a binding order of a government body.

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

2.1 Physical access control

Measures to prevent unauthorised persons from entering data processing facilities where personal data is processed and used

2.1.1 **CC Outsourcing / (Virtual) Private Cloud**

The rooms of the data centre protect the Contractor's infrastructure against unauthorised access and, in addition, ensure the ready availability of the building's technical services for the operation of the computer centre.

The premises upon which the computer centres are located are subject to strict security specifications with regard to access rights.

Access to the computer centres is only permitted for authorised individuals through various, independent access systems.

All visitors to the computer centres are recorded by staff, noting the date and the time when the visitors enter and leave the premises. Furthermore, access to the premises is only granted for special authorised purposes and, insofar as necessary, instructions are issued with regard to the security requirements of the area and regarding emergency procedures. Authorisa-

tion for access to the computer centre requires a signed statement personally agreeing to abide by the code of conduct and guidelines within the computer centre areas.

At some sites, the works security service patrols the premises at irregular intervals; additionally all parts of the computer centre building are protected with burglar alarm systems. Camera monitoring also records the incoming and outgoing accesses to the computer centres around the clock.

Within the building, different security zones can be defined at various sites, examples here are a control station zone, server areas, data archive, segments of the Client. Access generally occurs by means of a personally assigned and controllable access card belonging to the authorised persons. Authorisation for the individual zones is secured through an authorisation process and is granted solely in accordance with the necessity for the business model.

Each external visitor is accompanied by an internal employee during the entire visit to the computer centre. Service providers are only permitted to stay in the rooms of the CC while being monitored.

2.1.2 **Services without direct CC connection**

The following physical security measures apply for all sites or processing activities without a direct CC reference.

Access controls guarantee that only authorised company employees are admitted. Authorised access to offices, depending on the site, occurs during normal working hours through isolation sluices, a second security door, sets of dedicated locks, lock cylinders, door transponders, authorised employee IDs (RFID identification), automated access control systems (card reader) with personalised access cards, access keys for authorised internal employees. The issuance of keys is documented in a key book.

Visitors are picked up at the entrance by a contact person and accompanied in the facility during the entire stay.

At times the works security service patrols the premises at irregular intervals or parts of the building are protected with burglar alarm systems. At some sites camera monitoring for interior and exterior facilities also records the entrance area, the lobby, the lift systems as well as the accesses to the office areas around the clock.

2.1.3 **Public Cloud**

At some cloud providers the buildings are cared for and monitored by security staff and in the case of sensitive areas are also monitored with video.

There exists an access authorisation concept that is based on both a lock system, partially with a proper key administration, as well as an electronic access control system.

Admission to individual production areas and to the business area is restricted by means of an electronic access control system while using, for instance, magnetic cards.

Visitors are only permitted admission to sensitive areas after advance registration. In the course of accreditation, the visitor receives an identification, e.g. a visitor ID, which labels him as a guest and which he must carry with him during his stay at the site. At some sites the handling of guests is defined by means of a guideline. Admission to the individual production areas is only permitted with the accompaniment of authorised staff.

2.2 Admission control

Measures to prevent data processing systems from being used by unauthorised persons

2.2.1 **CC Outsourcing / (Virtual) Private Cloud**

All systems and applications require authentication for use of the services.

Access to the processing systems takes place with an unambiguous personal user ID and a password. The password is allocated in conformity with the password guidelines. To be mentioned here, for instance, are: requirements for password strength, forced password changes or the blocking of the user account after multiple log-ons with the wrong password to avoid risk (to prevent brute-force attacks).

A starter-changer-leaver process is carried out for employees. In this case authorisation is granted by the responsible management to carry out a user control on the basis of the "least privilege principle".

System administration and regular users receive separate user accounts. A check is also regularly done as to whether authorisation exists for privileged rights.

For remote access to the network, the use of 2-factor authentification methods (Secure ID cards or certificates) is prescribed in the information security guideline to avoid risk.

The protection of all networks against external access is regulated by firewalls and occurs by default over a security infrastructure chain made up of a proxy, virus scanner and firewall. At some sites, the special role of the Network Security Officer can be responsible for this.

It is possible to make an Intrusion Prevention System (IPS) available to actively fight against network attacks (Remote Access, Access Control lists, special WAN areas, etc.), which after being ordered is defined and included in the price in the service certificates for the various processing activities.

2.2.2 **Services without direct CC connection**

A starter-changer-leaver process is carried out for employees. In this case authorisation is granted by the responsible management on the basis of the "least privilege principle".

Access to the processing systems takes place with an unambiguous personal user ID and a password. The password is allocated in conformity with the password guidelines. To be mentioned here, for instance, are: requirements for password strength, forced password changes or the blocking of the user

account after multiple log-ons with the wrong password to avoid risk (to prevent brute-force attacks).

A check is regularly done as to whether authorisation exists for privileged rights. System administrators and regular users receive separate user accounts.

For remote access to the network, the use of 2-factor authentification methods (Secure ID cards or certificates) is prescribed in the information security guideline to avoid risk.

The protection of all networks against external access is regulated by firewalls and occurs by default over a security infrastructure chain made up of a proxy, virus scanner and firewall. At some sites, the special role of the Network Security Officer can be responsible for this.

2.2.3 **Public Cloud**

Regulations exist for access to IT systems.

These regulations (e.g. the password convention) requires among other things a minimum length and requirements for passwords (e.g. large and small case letters, numbers and special characters, maximum validity period, check for trivial passwords).

The logging on and off of users on the IT systems are logged.

The systems are to be locked or powered down when leaving the workplace. If this is forgotten, the workplace will lock automatically.

In addition there exists an admission authorisation concept. In general, all authorisations are withdrawn and must be activated again. The admission authorisation concept is based on the principle of user roles and profiles. The granting of personalised authorisations occurs through the responsible department.

Upon request, excerpts and summaries from the corresponding regulations can be made available.

2.3 Access control

Measures ensuring that those authorised to use a data processing system may only access data for which they have access rights and that personal data cannot be read, copied, modified or removed without authorisation when being processed and used and after being saved

2.3.1 **CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection**

Access control is based on a role-based authorisation concept for system accesses and graduated administration rights, in line with the task areas. All administrative activities are in principle logged on the systems and thus can be tracked. The access rights are allocated according to the minimal principle / "need-to-know" principle. Only as many access rights are granted as the job requires. Compliance with the "need-to-know" principle is the responsibility of the authorised executive.

When setting up an access, the user only receives minimal default authorisations. These may only be expanded over established application channels, whereby the respective line managers or responsible parties must give their approval for it to comply with an appropriate separation of functions in the authorisation process (dual control principle).

Remote access occurs over a VPN (virtual private network) connection or encrypted to the terminal server.

2.3.2 **Public Cloud**

There exists an authorisation concept for access to the IT systems.

The objective is to provide a secure, well-structured and uniform release and authorisation strategy on all IT systems. Accesses occur according to the “least privilege” concept.

Only authorised storage media is to be used. Employees of the cloud provider are subject to advanced restrictions and approval requirements to store personal data of the Client on mobile data media or to process same outside the cloud provider's business premises or to access same from there.

Access to the individual systems is controlled with special network authorisations and a client-based role concept (e.g. administrator, IT etc.). Access rights are documented accordingly. Access authorisations are withdrawn or deleted.

The cloud provider informs his staff about all relevant processes and role concepts and describes the consequences of violating the corresponding specifications.

Upon request, excerpts and summaries from the corresponding concepts can be made available.

2.4 Disclosure control

Measures ensuring that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during transport or when being saved on storage media and that it can be checked and established to which bodies personal data is intended to be sent through data transmission facilities

2.4.1 **CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection**

To reduce the risk for those impacted, employees are instructed to only use secure data transmission channels that are defined as obligatory in the data protection guideline. The possible data transmission can occur over trustworthy lines and networks which do not easily allow logging.

Different options, such as the use of SSL certificates for an encrypted Web communication, SSL virtual private network for a secured connection (secured remote access), electronic signature, logging, can be implemented upon request and documented and assessed in the service certificates.

In the meaning of order processing, the Client alone decides which data are to be transmitted, which transmission channel and which type of transmission are to be implemented. Network segments can also be insulated from one another here through access control lists and the entire network can be secured through multi-level firewall systems. If a data line that is not trustworthy has to be used for transmission, the transmission can also occur encrypted (e.g. via Virtual Private Network - VPN, Transport Layer Security - TLS, etc.).

For backing up data, mobile data media are used that are subjected to an automatic inventory-taking and stored in a secure area.

To guarantee transport control, a transport or sending of data media occurs only if this was the instruction of the Client. The Client also determines the transport method, which for instance comprises the sending by registered mail/insured parcel or the use of secured/locked transport containers and special courier services (encrypted sending). This is subject to a control and documentation process.

A necessary destruction of data media occurs through a specialised and certified company according to current norms. Up to destruction, the data media are stored in a security area and are protected from unauthorised access. The destruction of the responsible party's storage media and the making of records confirming that this destruction has taken place is only carried out in accordance with the order and instructions.

The code of conduct for the use of mobile data media (USB stick, CD, DVD, etc.) exists in the information security guideline. They ensure that personal data or operating and business documents may only be filed encrypted on mobile data media. This prevents the unauthorised reading, copying, modifying or deletion of data media within the scope of data media control.

A code of conduct exists for the secure destruction or the disposal of data media and confidential documents.

2.4.2 **Public Cloud**

Data transmissions occur within the secured network (e.g. with the corresponding encryption). The electronic transmission of data on public channels or over public networks takes place solely on encrypted channels. Various procedures are applied in coordination with the recipients.

The use of portable devices (e.g. their connection with a system) is subject to special regulations. No longer needed devices are disposed of in an appropriate way while observing the protection of personal data (e.g. physical destruction). In addition, various protective mechanisms are used to protect the databases (e.g. firewalls, regulations on specific procedures in the case of incidents). Upon request, excerpts and summaries from the corresponding concepts can be made available on the corresponding procedures.

2.5 Separation control

Measures ensuring that data collected for different purposes can be processed separately

2.5.1 **CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection**

A separation of the data occurs upon the instruction of the Client for his data. The different options will be defined and assessed in the service certificate for the various processing activities.

What can be named as examples for a logical or physical separation on the client and/or data level are: the separation of functions production / integration / test, use of various databases, use of access control software and set-up of access rights (with their logging), various encryption for individual datasets, logical separation (e.g. on shared systems), physical separation (e.g. on dedicated systems), etc.

With a remote activity the employee is accessing the already specified infrastructure, which allows him to process within the scope of previously established specifications.

2.5.2 **Public Cloud**

Based on the authorisation concept, measures such as directories are set up on the systems that guarantee a strict separation of data and files from other clients. Customer access to instances that do not correspond to the access authorisations is effectively prevented.

Test, productive and integration systems are operated separately from one another.

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

3.1 Input control

Measures ensuring that it can later be checked and established whether personal data has been entered in data processing systems, modified or removed from such systems and by whom this has been done

3.1.1 **CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection**

Input control as well as the retention period of the data thus generated occurs upon the instruction of the Client for his data and on his infrastructure or in his applications.

Optional logging as well as revision-proof storage of the logs can be implemented upon instruction and must be defined within the scope of the service certificate.

Administrative access to systems can be tracked through standard logging on the level of the operating system. This serves as proof of an unauthorised change or deletion of stored personal data within the scope of storage control.

An evaluation of the input control occurs only if needed within the scope of the instruction by a manual or automated log assessment.

3.1.2 **Public Cloud**

To the extent the input, change and deletion of data occurs on IT systems, the changes to this data is logged by means of the corresponding logging and log assessment systems (e.g. access ID, access time, authorisation and corresponding activity).

Upon request, excerpts and summaries from the corresponding concepts can be made available on the corresponding procedures.

3.2 Organisational and technical securing of authorisations, logging measures, log assessments /revision etc.

Additional explanations on the securing of authorisations are documented in detail in the chapter on admission and access controls. Log assessments are to be requested as part of the instruction and will be conducted in this scope. A specification is to be included in the respective service certificate.

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

4.1 Availability control

Measures ensuring that personal data is protected against accidental destruction or loss

4.1.1 **CC Outsourcing / (Virtual) Private Cloud**

All installations at the computer centre are physically protected against security threats and environmental risks.

Different graduated security facilities to ensure availability can be defined and specified for the business model in the service certificate.

Here are a few options: redundant electricity supply, highly available electricity supply (partially secured by USV) with static transfer switches (STS), diesel generator sets for the emergency electricity supply, air conditioning with high availability, fire alarm systems with early fire detection and direct alarm message to the local fire service, each computer centre its own fire compartment, burglar alarm system with door close control, emergency concepts and breakdown plan, redundant network connections and network infrastructure, clustered systems or redundant hardware (from construction elements to entire servers – geo-redundancy).

These security installations are regularly checked for reliability and fault tolerance.

Optionally, collaboration with external computer centres is possible upon instruction via service sub-providers; they are then available for the test operation, redundancy concepts (geo-redundancy) on the application level (through clusters, separation of computer centres, separate data mirrors etc.).

For a complete backup, depending on the specific purpose of the respective processing, various archiving options are available, e.g. a regular automatically initiated and monitored data backup (usually once per calendar week a full backup, daily incremental backups). The normal holding period of these backups is implemented upon instruction and documented in the service certificate. The data backup can occur in a separate backup system that is located in a different fire protection compartment or at a different site such as the productive system.

Virus protection is used on all Arvato Systems workplace computers. The presence of virus protection, as well as the regular updating of the virus definitions is ensured through the use of a centrally controlled client antivirus and firewall solution.

The timely loading of security updates for the operating systems and application programs used is prescribed by means of the corresponding Group policies and ensured by monitoring patch levels.

Topics dealing with BCM (Business Continuity Management) are described in more detail in the chapter on Incident Response Management.

4.1.2 **Services without direct CC connection**

The processing of data by employees occurs via remote / WLAN in the relevant Client computer centre and is thus also subject to the availability of this computer centre.

All employees are subject to the instruction of not storing activity-relevant data on a notebook, but rather to use backup-secured file areas set up for this purpose in order to exclude the risk of data loss.

4.1.3 **Public Cloud**

A backup concept exists. In these documents the measures for securing personal and company-critical data are described.

A regular complete backup is part of this. In addition, electronic images of the respective facility are created at regular intervals and, if necessary, after the installation of new data processing facilities and after far-reaching changes to the attachment of a facility.

The data backups, depending on the process or relevance, will be outsourced to other buildings or externally. An uninterruptible power supply will be set up.

Furthermore, corresponding emergency and business continuity plans exist for facilities of the cloud provider.

Upon request, excerpts and summaries from the corresponding concepts can be made available on the corresponding procedures.

4.2 Order control

Measures ensuring that personal data subject to contract data processing can only be processed in accordance with the Client's instructions.

4.2.1 CC Outsourcing / (Virtual) Private Cloud / Services without direct CC connection

The data will only be processed in accordance with the instruction of the Client. These instruction are to occur at the minimum in text form and solely by authorised persons of the Client to authorised persons of the Contractor.

All employees are obligated to data secrecy, as well as to special obligations such as the secrecy of telecommunications and social secrets. Inspection shall enable random checks to be carried out.

Computer centre inspections or audits are possible in the relevant computer centres according to proportionality and timely written registration with the responsible department. The organisation and execution of an audit is subject to the audit guideline for the protection of the personal data of various responsible parties.

4.2.2 Public Cloud

The service provider has appointed a company data protection officer and provides for their appropriate and effective integration into the relevant operational processes through the data protection organisation.

Employees are instructed about their roles and responsibilities e.g. by way of preparatory training sessions. The Client has appointed one or more responsible parties to control and monitor the data security specifications.

Documents on data protection and data security, responsibilities and relevant procedures are maintained and reviewed.

At regular intervals the Group audit department (IT and commercial audit) carries out extensive controls within the affiliated companies (pursuant to the definition of §§15ff Companies Act (AktG)). At regular intervals Compliance Management carries out extensive controls within the affiliated companies (pursuant to the definition of §§15ff Companies Act (AktG)).

Corresponding agreements are concluded with external service providers. Contract execution is tracked and controlled by the corresponding controls.

5 Process for regularly testing, assessing and evaluating (Art. 32 (1) lit. d GDPR; Art. 25 (1) GDPR)

5.1 Data protection management at the Arvato Systems Group

An external data protection officer was appointed for all legal units of the Arvato Systems, in which the core business of executing processing procedures with personal data or special categories of personal data pursuant to Article 9 GDPR or personal data regarding criminal convictions and offences pursuant to Article 10 GDPR occurs. A team of trained data protection officers is available at the email address Datenschutz@arvato-systems.de as a contact person in the role of data protection coordinators.

Arvato Systems defines the key features of data protection in the Group data protection guideline, as well as more specifically in the Arvato Systems internal data protection guideline.

Audits are carried out at regular intervals by the data protection officer and the IT audit department to test, assess and evaluate the effectiveness of the above-named measures. Within the scope of proportionality, a control option exists within the scope of an audit by the Client after timely advance notice.

As proof, Arvato Systems can provide the following certifications as evidence for a security-relevant processing activity: ISO / IEC 27001.

An ESAE report as proof of a proper processing activity and the observance of information security can be acquired at Arvato Systems.

The Arvato Systems security concept is enshrined in the Group guideline on the Information Security Policy.

The internal data protection guideline of Arvato Systems with an approved code of conduct is to be adhered to by all employees to increase the level of protection when processing personal data for those impacted. In addition, the risk is guaranteed by effective patch management, penetration tests, log analyses, dealing with Web security (e.g. OWASP) and via an SOC centre. A risk-based approach is preferred for the technical organisational measures.

Guaranteeing a procedure for regularly testing, assessing and evaluating the effectiveness of the technical organisational measures and the security of processing occurs via the following PDCA cycle with Plan (develop a security concept), Do (introduce TOMs), Check (monitor the effectiveness / completeness) and Act (continuous improvement).

The transmission of personal data to a third country occurs in coordination between the Client and the Contractor with the help of standard data protection clauses.

In his own area of responsibility the service provider ensures implementation of data protection management comparable to the protection level of Arvato Systems.

5.2 Incident Response Management at the Arvato Systems Group

Measures to quickly re-establish the availability of personal data and access to it after a physical or technical incident

Procedures are documented within the scope of the established BCM (Business Continuity Management) to ensure the continuation of business operations during an emergency or major disruption as well as to re-establish all services to be

provided to the Client as quickly as possible. Restarting exercises are conducted regularly.

Measures that ensure the resilience of the systems and services are designed in such a way that also selectively high loads or high continuous loads of processing remain feasible. Topics regarding the storage, access and line capacities, as well as backup and redundancy concepts, are included in more detail in the availability control.

5.3 Privacy-friendly default settings (Art. 25 (2) GDPR) at the Arvato Systems Group

The implementation of data protection is accompanied in product development by the consideration of an internal White Paper “Data protection in product development”, as well as a checklist for the consideration of data protection through technology design and privacy-friendly default settings.

Use of the White Paper is specified as mandatory in the data protection guideline of Arvato Systems.

Annex 2

Change history of this order processing agreement

Document	Date of entry into force	
Version 3.0	01.11.2018	A new point 5.2 and a new point 5.3 have been inserted; the numbering of the following points has been adapted. 5.2 The Client has knowledge of these TOMs. The Client bears sole responsibility for ensuring that they provide a level of security appropriate to the risks applicable to the Personal Data to be processed. 5.3 He agrees to indemnify, defend, and hold harmless the Contractor from and against any and all third party claims resulting from or related to the fact that these TOMs are not sufficient to ensure an appropriate level of security.