Special requirements for outsourcing to subcontractors

Bitte Ort auswählen, TT. Monat 2025

Introduction

Arvato Systems is a service provider for customers who are subject to state supervision by the Federal Financial Supervisory Authority (BaFin) and the Deutsche Bundesbank (Bundesbank). Due to these circumstances, insurance companies, banks, payment institutions, and other financial service providers (hereinafter referred to as "regulated companies") have special requirements for the outsourcing of services to third parties. The requirements imposed on Arvato Systems by regulated companies are set out below and must be observed throughout the entire service chain in the event of outsourcing, including by Arvato Systems' subcontractors. In such cases, the subcontractor shall therefore provide its services in such a way that Arvato Systems is able to comply with these requirements with regard to the subcontractor's services.

The following must also be observed with regard to the requirements set out below:

- "Client" refers to the regulated company for which Arvato Systems provides services that qualify as outsourcing. In the relationship between Arvato Systems and the subcontractor, Arvato Systems also has the rights of the client vis-à-vis the subcontractor; Arvato Systems can assert these rights for itself and/or the regulated company. In addition, the Regulated Company remains entitled to assert the rights of the Client directly against the subcontractor.
- "Contractor" refers to Arvato Systems, which provides services for a regulated company that qualify as outsourcing. In the relationship between Arvato Systems and subcontractors, the subcontractor has the obligations of the Contractor.

Special requirements for outsourcing on the part of the Regulated Company:

1 Preambel

With regard to this outsourcing, the client must in particular ensure compliance with the special requirements arising from the supervisory provisions – in particular Section 25(b) of the German Banking Act (KWG), Section 32 of the Insurance Supervision Act (VAG) and/or Section 26 of the Payment Services Supervision Act (ZAG), the current guidelines on outsourcing published by the European Banking Authority (EBA) (EBA/GL/2019/02) and the current guidelines on the management of ICT and security risks (EBA/GL/2019/04) in accordance with Directive (EU) 2015/2366 (PSD2) in conjunction with EBA/GL/2017/17 (Guidelines on security measures under PSD2) (hereinafter collectively referred to as "regulatory law"). In this annex, the Client and the Contractor wish to set out the necessary rights of the Client and obligations of the Contractor as an outsourcing company, as required to comply with the relevant regulatory obligations. This annex thus supplements the contract and takes precedence over it, unless otherwise specified.

2 Subject matter and scope of the outsourcing

It is the intention of the parties that the Contractor shall provide the agreed services and, in doing so, shall comply with the specific regulatory requirements applicable to the Client, as defined in more detail in this Annex.

If the Contractor is based outside the European Economic Area or the European Union, it shall appoint a domestic (i.e., Germany-based) authorized representative to whom BaFin can send notifications and deliveries directly. The Contractor shall immediately inform the Client in writing of any change in the authorized representative, stating the new authorized representative and their contact details. At the same time, the Contractor shall ensure in its agreements with subcontractors approved in accordance with Section 9 who are not resident in Germany that they also appoint an authorized representative and that the Contractor is informed immediately of any changes to this authorized representative in accordance with the above provisions. The Contractor shall immediately inform the Client of the authorized representatives appointed by its subcontractors and of any changes.

3 Control and ongoing monitoring

The parties agree that the outsourcing of the contractual services to be provided by the Contractor shall not impair either the management and control of these services by the Client or the fulfillment of regulatory obligations. The Contractor shall therefore enable the Client, the competent authorities, and external auditors to continuously monitor and assess the performance of the

tasks outsourced to the Contractor and its subcontractors in accordance with the following provisions. This includes, in particular, the right to inspect and enter business premises and the Contractor's obligation to provide relevant information and documents.

The respective designated contact persons of the parties are responsible for implementing this outsourcing and for controlling and monitoring the outsourced activities. The Client and the Contractor shall designate the respective contact persons (and at least one deputy in each case) and provide them with sufficient authority to perform their tasks. Any personnel changes relating to one of the designated contact persons must be communicated to the other party one (1) month before the change takes effect, if possible. In this context, a new contact person must be designated. If prior notification is not possible, the other party must be notified immediately (within one (1) working day at the latest) after the personnel change becomes known.

The Contractor further acknowledges that, in the performance of its services, it is subject to ongoing monitoring by the Client as part of the Client's internal control procedures. Internal audit officers or other internal control functions of the Contractor shall cooperate with the Client in a spirit of trust. Reports from the internal audit department or other functions of the Contractor regarding the outsourced activity shall be forwarded to the Client, in particular for the purpose of checking identified deficiencies.

4 Authority to issue instructions

The Contractor shall perform the contractually agreed services on its own responsibility. However, the Client shall be entitled at any time, directly and independently of any competing rights to issue instructions, to issue the Contractor with specific instructions in connection with the performance of this contract and in accordance with the obligations arising for the Contractor from this contract, insofar as this is necessary to ensure the proper performance of the outsourced activity and to monitor its execution.

The instructions must be in writing. In justified individual cases, instructions may also be given verbally by persons duly authorized by the Client. These must be confirmed in writing without delay.

The Contractor also acknowledges the corresponding rights of instruction of BaFin in accordance with supervisory law (e.g., Section 27 ZAG).

5 Agreed service quality and Reporting obligations

The Contractor shall comply with all current legal requirements (e.g., due to supervisory regulations) in relation to the outsourced activity.

The Contractor shall report to the Client regularly, at least quarterly, in writing (email is sufficient) on the outsourced activity. The relevant reports and the reporting period shall be agreed upon by the parties.

The Contractor shall also be obliged to inform the Client within a reasonable period of time of all significant errors and incidents in the performance of the services. Significant errors and incidents include, in particular, those that could lead to considerable damage or significantly impede the organizational workflow, intentional damage caused by employees, a accumulation of negligently caused disruptions, and personnel shortages that have a significant impact on the provision of services.

Where necessary, the Contractor shall inform the Client within a reasonable period of time of any reportable incidents, taking into account in particular the EBA Guidelines on reporting serious incidents pursuant to Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/10) and the BaFin Circular 08/2018 (BA) on the reporting of serious payment security incidents.

The decisive factor for the reporting obligation is whether the incident violates one of the protection objectives of confidentiality—including informational self-determination (data protection)—availability, reliability, or integrity. In particular, there is a reporting obligation in the following cases: Typical IT-related security incidents such as the occurrence of malware; unauthorized access to data; loss of data carriers; unauthorized access to security areas; disclosure of personal data; system interruptions.

The Contractor is further obliged to inform the Client of any developments that may impair the proper performance of the outsourced activity. In particular, the Contractor shall immediately inform the Client in a manner appropriate to the specific situation of any circumstances that may have an impact on the agreed quality of service or on the compatibility of the service provision with the applicable legal and/or regulatory requirements. Upon request by the Client, the Contractor shall be obliged to provide the Client with the relevant information.

The parties undertake to implement changes to the agreed quantitative and qualitative performance targets if this becomes necessary due to changes in the legal framework, including the administrative practice of BaFin or a request from BaFin or another competent authority. In this case, the parties shall immediately amend the contract and relevant annexes in accordance with the necessary changes.

6 Contractor's location(s), data and system security

The Contractor shall provide the contractual services at its headquarters in Germany. The relevant data of the Client shall be stored and processed exclusively at its headquarters in Germany. The Contractor shall inform the Client immediately, at least thirty (30) days before it intends to provide the contractual services or parts thereof at a location other than the one agreed for the specific service. The Client may object to such a change of location within fourteen (14) days of being informed, provided that this would seriously jeopardize the fulfillment of the contractual obligations.

The Contractor shall maintain banking secrecy and treat the Client's data as strictly confidential, protect it, and comply with all data protection requirements applicable to the Contractor and the Client, in particular those of the EU General Data Protection Regulation (EU) 2016/679, and ensure the confidentiality, integrity, availability, authenticity, and continuity of the data. "Data" within the meaning of this contract refers to all data of the client, in particular personal and sensitive data, such as customer data, user and end-user data, as well as data that is collected, used, processed, stored, or created under the contract. All rights to and power of disposal over the data remain exclusively with the client, regardless of the form of processing by the contractor. The Contractor guarantees that only employees of who are bound to secrecy have access to the Client's confidential information. Unless a party is subject to a legal disclosure obligation or unless otherwise agreed in this annex, in particular in section10 , no party may disclose the confidential information to third parties or otherwise disclose it without the prior consent of the other party.

The Contractor shall implement and maintain appropriate IT security standards and data protection mechanisms in accordance with generally accepted standards (e.g., ISO 27001 and ISAE3401) to ensure data and system security and prevent unauthorized access to or loss of data. The Contractor shall ensure the proper performance of the outsourced tasks, in particular through ongoing internal controls of the services provided.

The Contractor warrants that its IT security standards and data protection mechanisms comply with the Guidelines on the management of ICT and security risks (EBA/GL/2019/04).

The Contractor shall ensure that sufficiently trained and qualified personnel are employed for the outsourced activity.

If the contractual services of the Client also include the processing of data within the meaning of the GDPR, this is also subject to the provisions of the data processing agreement concluded between the Contractor and the Client.

The Contractor shall retain all documents relating to the outsourced activity in accordance with the retention periods applicable under commercial law and other applicable laws and shall take the necessary precautions to ensure that no data relating to the outsourced activity is lost.

In the event of its insolvency, the winding up or cessation of its business activities, and in the event of a corresponding instruction by the Client, the Contractor shall ensure that the Client has unrestricted access to all documents and data subject to the Client's power of disposal.

7 Implementation and testing of contingency plans

The Contractor shall have a risk and business continuity management system in place, including a documented emergency plan with business continuity and recovery plans in accordance with Annex A for all events that could affect the Contractor's performance (including events of force majeure). The emergency plan must ensure that replacement solutions are available in a timely manner in the event of an emergency. The recovery plans must enable a return to normal operations within a reasonable period of time. The communication channels to be used in an emergency must be specified.

The emergency plan shall be made available to the Client at any time upon request. The Contractor is obliged to test and trial the emergency plan regularly, at least once a year.

Insofar as the outsourced activity is affected, the Contractor shall notify the Client of the emergency and recovery plan drawn up in accordance with Annex A and any updates thereto within a reasonable period of time.

8 Insurance

For the duration of the contract, the Contractor undertakes to maintain adequate insurance coverage customary in the industry for the contractual services with a reputable European insurance company, in particular liability insurance coverage. At the request of the Client, the Contractor shall submit the insurance policies to the Client.

9 Subcontracting

Any transfer of individual or all contractual services of the Contractor, as well as any significant change to an existing transfer, is only possible with the prior written consent of the Client, whereby the Client will only refuse consent for objective reasons. An objective reason shall be deemed to exist in particular if there is justified cause for doubting that the subcontractor will perform the services properly, compliance with the obligations specified in this Annex cannot be ensured, or a competent authority denies the permissibility of the transfer for any reason whatsoever.

The Client shall have the right to revoke its consent to subcontracting at any time if there is an objective reason for doing so. In this case, the Contractor shall be obliged to immediately release the subcontractor from the performance of the subcontracted work and to provide the Client with evidence of this release upon request.

The Contractor shall inform the Client in writing in good time before the planned outsourcing or planned change to an existing outsourcing arrangement and, at the Client's request, shall submit the (amended) outsourcing agreement; this information shall include at least a description of the subcontractor, the type of outsourced activity, the duration of the planned outsourcing and the planned location of service provision. The information must be provided no later than thirty (30) days before the planned outsourcing or planned change to the existing outsourcing takes effect in order to enable the Client to carry out an adequate risk assessment and make an informed decision on the approval of the planned outsourcing or planned change to the existing outsourcing.

The Client shall notify the Contractor of its approval or rejection of the planned transfer or planned significant changes within thirty (30) days of receipt of the notification. Rejection may only be based on reasons arising from the risk analysis and giving rise to concerns about an adverse effect on the implementation of this outsourcing.

The Contractor undertakes to conclude a sub-outsourcing agreement with the subcontractor in accordance with the provisions of this Annex. In its sub-outsourcing agreement with the subcontractor, it shall in particular ensure that (i) the subcontractor undertakes to comply with all applicable laws, regulatory requirements and obligations under this Agreement, and (ii) the Client and BaFin or other competent authorities and auditors appointed by them are granted the same direct rights, including rights of access and inspection, as those granted by the Contractor in accordance with sections3 ,4 , and10 of this Annex.

Even in the event of subcontracting, the Contractor shall remain fully responsible for compliance with the contractual obligations. It shall therefore continuously monitor the subcontractor with regard to the subcontracted services and ensure regular reporting on compliance with the relevant KPIs and SLAs in order to guarantee that all its obligations under this contract are continuously fulfilled.

The above provisions shall apply mutatis mutandis to the further transfer of services by subcontractors of the Contractor or their subcontractors.

10 Right of access and inspection

The Contractor shall grant (i) the Client, in particular the Client's internal audit department, (ii) the internal audit department of Bertelsmann SE & Co. KGaA, (iii) the Client's auditors, and (iv) the competent authorities of the Client, in particular BaFin and the Bundesbank, or (v) auditors commissioned by the competent authority, BaFin or the Bundesbank, full and unrestricted rights of

information, inspection, audit, access and access rights (access and audit rights) with regard to the services provided under the contract at any time in accordance with the following provisions:

The Contractor grants the right of access and inspection (i) to the relevant business and operating facilities relating to the Client, including business premises, data centers, IT systems, devices, networks, information, and data used for the performance of the contractual services, (ii) with regard to the relevant documents (including financial information, personnel, and the Contractor's external auditors) and shall provide information to the extent necessary for the performance of the internal control procedures and audits required under supervisory law (e.g., Section 25b KWG or Section 26 ZAG) or other audits ordered by the authorities. The right of access and audit includes, in particular: the performance of on-site audits at the Contractor's premises, the preparation of copies of relevant documents, and access to all documents, data carriers, and systems at the Contractor's premises, insofar as these relate to the services for the Client, and the right to perform security penetration tests to evaluate the effectiveness of the measures and processes implemented in the area of cyber security and internal IT security. The Contractor hereby releases its employees, internal auditors, and auditors from any confidentiality obligations towards the above-mentioned persons.

The Contractor hereby declares that, within the scope of audits ordered by BaFin or other competent authorities vis-à-vis the Client, it will tolerate such audits in the area concerning the Client and further undertakes to cooperate fully with BaFin or other competent supervisory authorities or commissioned third parties and to provide all information and hand over all documents that they require for their supervisory activities.

The Client shall generally give four weeks' advance notice of an audit by letter, fax, or email. If, due to requirements imposed by an authority, only a shorter notice period can be given, the Client shall inform the Contractor as soon as possible.

The right of access and inspection under this section10 shall remain in force for at least two years after termination of the contract, beginning at the end of the fiscal year in which the contract ends. Notwithstanding other statutory retention periods (e.g., HGB, AO), relevant documents must remain available in the original or, if not available, in a copy for the same period of time, unless they are to be returned or destroyed upon termination of the contract.

11. Special termination rights and transfer of the outsourced function(s) to another service provider or reintegration

The following shall be considered important reasons entitling the Client to terminate the contract:

- the Contractor violates applicable law, legal provisions, official requirements, or contractual provisions;
- the Contractor undertakes an impermissible further transfer in violation of the provisions of9 ;
- significant obstacles are identified that could significantly alter or prevent the performance of the outsourced function;
- significant changes occur that have a significant impact on the contract or the Contractor (such as subcontracting or changes to the Contractor's subcontractors);
- significant deficiencies arise with regard to the handling and security of confidential, personal, or otherwise sensitive data or information;
- the Contractor fails to comply with the access and inspection rights set out in section10 ;
- Instructions are issued by BaFin or another authority responsible for the Client and the Client can no longer use the services under this contract in the same manner, or if the competent authority demands the termination of this contract or individual services provided under this contract (e.g. if the competent authority is no longer able to effectively monitor the Client).

In the event of non-renewal, termination, or other termination of the contract, the Contractor shall support the Client in transferring the function(s) outsourced under the contract to another service provider or reintegrating them into the Client (**"Exit** Services"). To this end, the parties agree as follows:

- Upon notification of non-renewal, termination, or other termination of the contract (including termination by the Contractor) ("Exit Event") or from the date on which the Client so requests, the Contractor shall provide the Client or a third party named by the Client with the reasonable assistance requested by the Client to enable an orderly transfer of the

outsourced function (including all data processed under the contract) to a third party or the retransfer to the Client without interruption or impairment of the contractual services ("Exit Services").

- The Contractor shall provide the Exit Services until at least the effective date of the termination or expiration of the contract or, at the Client's option, for up to a maximum of [eighteen (18)] months after the occurrence of the Exit Event. The provision of Exit Services by the Contractor shall be subject to the provisions of the contract. In case of doubt, remuneration for Exit Services shall be based on the contract, unless the parties have agreed otherwise in the event of an exit.
- For the duration of the Exit Services, the Contractor shall not replace any of its employees who provide the Exit Services for the Client without the prior written consent of the Client.
- All relevant provisions of the contract shall remain in force for the duration of the provision of the exit services.
- Upon the occurrence of an Exit Event, the Client shall have the option, at its sole discretion, to request a temporary extension of the contractual services provided by the Contractor at the terms and conditions applicable at that time for up to six (6) months from the effective date of the Exit Event. To this end, the Client shall notify the Contractor in writing of this option at least thirty (30) days prior to the effective date of the Exit Event. In such a case, the term for the duration of the exit services provided by the Contractor shall be calculated from the date of expiry or termination extended in accordance with this clause.
- At the request of the Client, the Contractor shall develop a draft exit plan within a period to be agreed between the parties and make it available to the Client. The exit plan shall describe the exit services to be provided and the framework for the orderly transfer of the outsourced function to a third party named by the Client or to the Client, including the handling and migration of the data processed under the contract. The parties shall negotiate the details of the exit plan and finalize it as soon as possible after the contractor has submitted the first draft and sign it as a further annex to this contract.

Upon termination of the contract, the Contractor shall return all documents in its possession belonging to the Client, as well as files containing the Client's data, to the Client or to a third party designated by the Client. Files shall be made available in a form that allows the Client to read and process them with reasonable effort. If data formats are adapted to the Client's individual needs, the Contractor shall provide the Client with documentation of these adaptations. The Contractor is not entitled to retain copies of documents or data and is obliged to delete them completely and irrevocably, unless this constitutes a violation of legal regulations.

.

Annex A - Business Continuity Management

1. Introduction

The parties agree on the present Business Continuity Management (**BCM**), which sets out regulations for maintaining business operations with regard to the cooperation between the client and the contractor. The BCM is based on a framework for the management of operational and security-related risks of the client.

2. Risk analysis

The Contractor shall carefully analyze the extent to which it is at risk from serious operational disruptions and shall assess their potential impact quantitatively and qualitatively on the basis of internal and/or external data and a scenario analysis. The Contractor shall consider a range of different scenarios, including extreme but conceivable scenarios to which it may be exposed, and shall assess the possible impact of these scenarios.

3. Business continuity measures

The Contractor shall implement reliable business continuity measures to limit losses in the event of serious operational disruptions.

Based on the risk analysis performed, the Contractor shall, in particular, implement emergency and recovery plans so that the Contractor (i) can respond appropriately to emergencies, (ii) can maintain essential business activities in the event of an interruption to normal business operations, and (iii) can resume normal business operations within a reasonable period of time.

The Contractor shall ensure that the emergency and recovery plans (i) take into account the impact on the performance of the outsourced activity and are coordinated with the Client's emergency and recovery plans, and (ii) are documented, made available to the business and support units, and are easily accessible in an emergency.

4. Testing and updating emergency and recovery plans

The Contractor shall test the emergency plans regularly, at least annually, for their effectiveness and adequacy, and shall analyze and document any resulting problems and errors.

When testing its business continuity plans, the Contractor shall (i) include an appropriate set of scenarios, (ii) design the tests in such a way that the assumptions on which emergency plans are based, including corporate governance arrangements and crisis communication plans, are challenged, and (iii) include procedures for reviewing the ability of its employees and processes to respond appropriately to the above scenarios.

The plans should be updated at least annually and, if necessary, after changes to systems and processes. This update must be carried out in accordance with the test results obtained, new information about risks and threats, lessons learned from previous incidents, and changed recovery objectives, and in coordination with the AG's contingency plans.

5. Crisis communication

In the event of a disruption or emergency and during the implementation of emergency plans, the contractor shall ensure that it has effective crisis communication measures in place so that all relevant internal and external parties, including external service providers, are informed in a timely and appropriate manner.