Annex

„Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector”

Bitte Ort auswählen, TT. Monat 2025

Introduction

Arvato Systems is a service provider for customers who are subject to state supervision by the German 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 be observed with regard to the requirements set out below:

- “Customer” refers to the Regulated Company for which Arvato Systems provides services that qualify as outsourcing. In the relationship between Arvato Systems and subcontractors, 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.
- “Service Provider” 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 Service Provider.

Annex „Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector”

1 Obligations of the Service Provider

The Service Provider is obliged to do the following as part of the provision of services under the Agreement:

1.1. The Service Provider has appropriate standards for information security and applies the latest and highest quality standards for information security, whereby in particular the information security standards implemented by the Customer must be complied with by the Service Provider (Customers Security Technical and Organizational Measures). [1]

1.2. If the Customer provides for ICT security awareness programmes and digital operational resilience training and the Customer requires the Service Provider's personnel to participate, the Service Provider shall participate in these training sessions. Participation in the training is free of charge, however the training time is not considered billable time. The Service Provider's personnel shall maintain confidentiality regarding the content of the training. At the request of the Customer, the Service Provider shall provide relevant personnel with appropriate evidence of participation in training courses on ICT security awareness programmes and digital operational resilience trainings conducted by the Service Provider itself or by third parties. [2]

1.3. Furthermore, the Service Provider and/or its Subcontractors – depending on for whom the certification is required for the provision of the respective service – undertakes to have the following certifications, to maintain these including their successor certifications and to submit evidence of the existing certifications to the Customer upon request: (i) ISO 27001 and (ii) ISAE 3402. The scope of the certifications must in any case include all parts of the Service Provider's organisation involved in the provision of the agreed services. The Service Provider must impose this obligation on the Subcontractors it uses by means of a written contract. [3]

If and to the extent that further certifications are required in the future for the provision of the service, these shall in any case be acquired by the respective Service Provider. In addition, the Customer may request that further certificates be obtained, whereby the Service Provider shall bear the costs for the certifications that are necessary for the provision of the service. The Customer shall bear the costs for any additional certifications, unless the Service Provider already holds these.

2 Support with ICT-related incidents [4]

2.1. The Service Provider shall inform the Customer immediately, proactively and in writing about ICT-related incidents and payment-related operational or security incidents within the meaning of the DORA Regulation that are related to the services of the Service Provider and/or its Subcontractors.

2.2. The Service Provider shall support the Customer in the event of an ICT-related incident within the meaning of the DORA Regulation in connection with the services of the Service Provider.

2.3. The Service Provider shall not charge any additional costs for support in the event of an ICT-related incident.

3 Use of Subcontractors [5]

3.1. The Service Provider shall generally provide the services under the Agreement itself. If the Service Provider intends to use third parties ("**Subcontractors**") for the provision of services that support critical or important functions or essential parts thereof, this requires the prior written authorisation of the Customer.

3.2. A list of current subcontractors must be specified by the service provider in the Agreement.

3.3. The use of Subcontractors for (partial) services under the Agreement is not permitted if:

- the Subcontractor has its registered office outside the European Economic Area;
- the outsourcing results in a data transfer outside the European Economic Area, unless this has been expressly authorized in advance in writing by the Customer, subject to any conditions; In any case, the specific requirements of the GDPR for data transfers to third countries (Art. 44 ff) must be fulfilled, such as the EU Standard Contractual Clauses (SCC) or other suitable guarantees.
- the Subcontractor is in competition with the Customer.

3.4. The Service Provider must inform the Customer in writing, with a reasonable lead time of at least 60 days, submitting all essential documents from the due diligence within the meaning of section 3.7 in sufficient quality, in particular the details of the scope of the planned use of the Subcontractor or change and the qualification of the Subcontractor ("**Notification**"). The Customer is entitled to object to the (change in) the use of the Subcontractor if this could impair the Customer's essential interests. This is the case if the Subcontractor is granted access to personal data, in the event of significant detrimental effects on the outsourcing relationship, in the event of an increase in risk or due to regulatory requirements. If the Customer does not object to a timely announced (change in) utilization of a Subcontractor within 60 days of receipt of the notification, this shall be deemed as consent. If an objection is raised in due time, the Service Provider is not authorized to implement the planned outsourcing or change.

3.5. In the event of changes to the approved Subcontractor or its services that lead to a significant increase in risk for the Customer, the Customer has the right to request changes to the proposed changes to the subcontracting before they are implemented.

3.6. The Customer may revoke consent and authorization of a Subcontractor for good cause at any time in the future.

3.7. In connection with the use of Subcontractors, the Service Provider must comply with the following minimum requirements prior to the use of the Subcontractor supporting critical or important functions or essential parts thereof and on an ongoing basis: [6]

- implementation and execution of a due diligence process that ensures that the Service Provider is able to assess the suitability of the Subcontractor for the provision of services. Due diligence must be carried out before the Subcontractor is engaged. Its scope must comply with the requirements of the technical regulatory standards pursuant to Art 28 para 10 and Art 30 para 5 DORA Regulation and include the following, among other things: assessment of the Subcontractor's capabilities, expertise and financial, human and technical resources (including through participation in operational reporting and operational testing as may be required by the Customer); assessment of information security standards, organisational structure, risk management and internal controls.
- assess all risks, including ICT risks, associated with the location of the Subcontractor and its parent company, if any, and the location from which the subcontracted service is provided (see Annex I); and provide relevant documentation on this risk assessment upon request of the Customer;
- definition of the Subcontractor's monitoring and reporting obligations, which the Subcontractor must fulfil vis-à-vis the Service Provider and thus also vis-à-vis the Customer;

- continuous provision of the service even if a Subcontractor fails to meet its service levels or other contractual obligations; and
- continuous compliance with the ICT security standards and, if applicable, the additional security features by the Subcontractor in accordance with the technical regulatory standards pursuant to Art 28 para 10 DORA Regulation.

3.8. The Service Provider must impose all obligations arising from the Agreement and this Supplementary Agreement on each Subcontractor in writing as part of the commissioning of the respective Subcontractor. The contract with the Subcontractor must ensure that the Customer and the relevant authorities can exercise their information, audit and instruction rights directly vis-à-vis the Subcontractor. The Service Provider must continuously monitor the Subcontractor's ongoing compliance with the Agreement and this Supplementary Agreement and provide evidence of this at the request of the Customer. [7]

3.9. The Service Provider must inform the Customer immediately, proactively and in writing of any developments at the Subcontractors that could have a significant impact on the proper provision of the services under the Agreement and this Supplementary Agreement. The Service Provider shall be liable for all Subcontractors as for its own actions. Furthermore, the obligations and responsibilities of the Service Provider arising from the Agreement and this Supplemental Agreement shall remain unaffected by any subcontracting. [8]

4 Locations of service provision and data processing [9]

4.1. The country where the service provider and its approved subcontractors provide the services and where they store and process the data must be documented in Annex 1. If the Service Provider or the Subcontractor intend to change these locations, the Customer must be informed in advance. In addition to this duty to inform, the Service Provider must fulfil the obligations set out in section 4.2.

4.2. The full or partial relocation of a place of performance, a place of data storage and processing or the registered office by the Service Provider or by the Subcontractor shall always require the prior written consent of the Customer.

5 Access to Data

5.1. In the event of insolvency, resolution, cessation of the Service Provider's business activities or termination of the Agreement or this Supplementary Agreement, the Customer shall be entitled to access its data immediately.

5.2. The Service Provider shall provide the Customer with comprehensive support and unrestricted access and ensure that the Customer's data is restored and returned in an easily accessible format as specified by the Customer. [10]

6 Emergency Measures

6.1. The Service Provider implements and tests its business contingency plans. Furthermore, the Service Provider shall have measures, tools and guidelines for ICT security that provide an appropriate level of security for the provision of services by the Customer in accordance with its legal framework.

6.2. The Service Provider shall document the implementation of the testing of the business contingency plans and make this documentation available to the Customer immediately upon request. [11]

7 Service Levels [12]

7.1. The service levels specified in the Agreement shall apply, which enable effective monitoring of the provision of services by the Customer. The service levels shall be reviewed by the Service Provider and the Customer as required to ensure that they are appropriate in the light of further developments in technical standards and shall be adjusted or supplemented as necessary. The Customer may request corresponding adjustments and additions to the service levels in any case if the agreed service quality is not achieved. The Service Provider shall comply with the corresponding requests of the Customer to adapt or change the service levels without undue delay and shall also immediately take the appropriate corrective measures taken by the Customer if the agreed service quality is not achieved.

7.2. The Service Provider must inform the Customer immediately, proactively and in writing of any developments that could have a significant impact on the proper provision of the services and/or the associated activities and processes in accordance with the agreed service levels. [13]

8 Information and Audit Rights [14]

8.1. The Service Provider grants the Customer, the commissioned third parties (e.g. internal and external auditors), the supervisory authorities and bodies and the Customer's resolution authority the following information and audit rights with regard to the services of the Service Provider and its Subcontractors during the term of the Agreement and after termination of the Agreement:

- unrestricted access, inspection, instruction and audit rights, including full access to all business premises, including the full range of relevant equipment, systems, networks, information and data used for the performance of the Services under the Agreement, including in connection with financial information, personnel and the Service Provider's external auditors; as well as access to employees, documents, data storage, business premises and systems at the Service Provider and its Subcontractors and the provision and transmission of information and documents. In particular, the Service Provider shall grant the Customer, the audit, supervisory and resolution bodies and authorities unrestricted and unhindered access to all records, information and data related to the services under the Agreement, in particular those necessary to ensure that the services comply with regulatory and data protection requirements.
- to grant unrestricted rights of inspection and audit in connection with the Agreement in order to enable the ongoing monitoring of compliance with the Agreement and to ensure compliance with the legal requirements and to cooperate fully in this regard.
- the right to make copies of relevant documents on site if they are of decisive importance for the business activities of the Service Provider;
- the right to agree alternative assurance levels if the rights of other customers are affected;
- the right to issue general guidelines and specific instructions to the Service Provider on the aspects to be taken into account when performing the services; 15
- the right that, where appropriate and necessary for supervisory purposes, the supervisory authority may address questions directly to the Service Provider, which must be answered by the Service Provider. 16
- the Service Provider's obligation to co-operate fully with on-site inspections and audits carried out by the competent national and European authority, the Customer or a contracted third party.
- the Customer shall give the Service Provider reasonable advance notice, if possible, of the details of the scope and frequency of the on-site inspections and the procedure to be followed. Audits may cover all areas relevant to the provision of services under the Agreement. In conducting these audits, the Customer shall comply with generally recognised audit standards in accordance with any supervisory instructions for the application and inclusion of such audit standards. 17

8.2. The Service Provider is obliged to co-operate fully with the authorities and resolution authorities responsible for the Customer, including persons designated by them. [18]

8.3. In addition to the audits, the Service Provider undertakes to participate in the vulnerability or threat-orientated penetration tests of the Customer and to cooperate fully in these. [19]

8.4. At the Customer's request, the Service Provider shall submit the following reports to the Customer: regular reports (including the Service Provider's internal audit report) and reports on (i) ICT incidents, (ii) the provision of services, (iii) ICT security, (iv) measures and tests to maintain operations, (v) audit reports from the Service Provider's external auditors. [20]

9 Termination [21]

9.1. The Customer is entitled to terminate for good cause the Agreement including this Supplementary Agreement or individual, definable partial services immediately or at a time specified by the Customer, in particular if one of the following events occurs: [22]

- Any material breach by the Service Provider of any applicable laws, regulations or the terms of the Agreement or this Supplemental Agreement;

- There are demonstrable weaknesses in the Service Provider's overall ICT risk management and, in particular, in the way in which it ensures the availability, authenticity, security and confidentiality of data, whether personal or otherwise sensitive data or non-personal data or information;
- Effective supervision of the Customer by the supervisory authority is no longer possible as a result of the terms of the Agreement and this Supplementary Agreement or the circumstances associated with these Agreements;
- Circumstances identified in the course of monitoring the ICT third-party risk that are deemed likely to affect the performance of the functions provided for under the Agreement and this Supplemental Agreement, including material changes affecting the Agreement or this Supplemental Agreement or the Service Provider's situation;
- in the case of use of a Subcontractor without the corresponding consent of the Customer or in the case of a significant change to the subcontracting without corresponding consent or in the case of use of a Subcontractor beyond the authorised scope of services. 23

9.2. The parties agree that they will work together – irrespective of the form of termination and the reason for termination – to achieve a proper termination and migration of the services to the Customer itself or to a third party designated by it.

To this end, the Service Provider shall provide the support services defined below for the transition (**"Termination Support"**) and, at the request of the Customer, extend the provision of services (**"After-Effect"**).

The Customer shall also be entitled to these rights in the event of merely partial termination of the Agreement.

9.3. The Service Provider's termination support shall include the provision of all support services that enable a smooth migration of the terminated services owed by the Service Provider under the Agreement to the Customer or a third party designated by the Customer from the date of termination until [12] months after the effective date of termination or after the end of any agreed After-Effect (**"Support Period"**). The Service Provider shall provide the Termination Support services at the written request of the Customer on the basis of the agreed commercial terms if the support services are provided as a result of termination for cause by the Customer, the Service Provider shall not be entitled to any compensation for its activities in order to minimise the Customer's loss. When providing the services, the Service Provider shall adhere to the Customer's schedule to the best of its ability.

At the request of the Customer, the Service Provider shall provide all services during the support period that are necessary or expedient for a smooth migration to the succeeding contractor.

9.4. If the Customer or the subsequent Contractor is unable to take over the provision of the Services after the termination of the Agreement, the Service Provider shall continue to provide all services on the basis of the Agreement for a maximum period of [24] months after the effective termination of the Agreement at the written request of the Customer.

10 Allocation of Rights and Obligations

A clear allocation of rights and obligations between the Customer and the Service Provider shall be made in writing in the Agreement, including any annexes, in order to comply with the applicable statutory and regulatory provisions for the entire duration of the Agreement. [24]

11 Amendments

11.1. Due to the fact that in connection with the implementation and interpretation of the DORA Regulation, delegated acts and further concretization by the competent European and national supervisory authorities are still to be expected, the contracting parties will monitor the corresponding requirements and inform each other accordingly.

11.2. In this context, the Service Provider undertakes to cooperate in the preparation of the new version or amendment of this Supplementary Agreement, in particular by providing the necessary information.

11.3. Irrespective of this, the Service Provider is in any case obliged to implement any necessary changes to the requirements and content, insofar as these are legally required. Otherwise, the Customer shall be entitled to an extraordinary right of cancellation.

12 Order of Precedence

12.1. The provisions of the Agreement shall continue to apply and this Supplemental Agreement together with its Annexes, which are an integral part of the Supplemental Agreement, merely supplements the applicable provisions of the Agreement.

12.2. In the event of inconsistencies, ambiguities or contradictions between the Agreement and this Supplementary Agreement, this Supplementary Agreement shall take precedence, unless stricter provisions contained in the Agreement are based on statutory regulations or regulatory requirements.

---

[1] This clause implements Art 28 (5) DORA Regulation.

[2] This clause implements Art 30 para 2 lit i DORA Regulation.

[3] This point implements Art 8 para 2 lit c DelR (EU) 2024/1773 (RTS specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers).

[4] This chapter implements Art 30 para 2 lit f DORA Regulation.

[5] The following section 3.1 implements margin no. 37 lit e EIOPA Guidelines (EIOPA-BoS-20-002) and Art 274 para 4 lit k DelVO 2015/35. In addition, this chapter amends Art 7 para 1, Art 3 para 1, Art 4, Art 6 Consultation Paper on RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Art 30 para 5 DORA Regulation ("**RTS on subcontracting**").

[6] This section 3.3 implements Art 3 and 4 Consultation Paper on draft RTS on subcontracting.

[7] This point implements Art 3 (1) lit c and Art 4 lit i RTS on subcontracting.

[8]This point implements margin no. 80 lit c EIOPA-BoS-20/600, Art 274 (4) lit c and l DelVO 2015/35 and Art 30 (3) lit b DORA Regulation.

[9] This capital implements margin no. 37 lit f EIOPA-BoS-20-002 and Art 30 (2) lit b DORA Regulation.

[10] Basically regulated in margin no. 37 lit n EIOPA-BoS-20-002, but concretised by Art 30 para 2 lit d DORA Regulation (in particular on the form of the return of data).

[11] This point implements margin no. 80 lit b EIOPA-BoS-20/600 and margin no. 37 lit l EIOPA-BoS-20-002 and Art 30 (3) lit c and Art 28 (8) DORA Regulation.

[12] This chapter implements margin no. 80 lit a of the EIOPA Guidelines on ICT Security (hereinafter "EIOPA-BoS-20/600"), margin no. 37 lit i EIOPA-BoS-20-002, Art 274 (4) lit f DelVO 2015/35 and Art 30 (2) lit e and (3) lit a **DORA** Regulation.

[13] This point implements margin no. 80 lit c EIOPA-BoS-20/600 and Art 30 (3) lit b DORA Regulation.

[14] This chapter implements margin no. 80 lit d EIOPA-BoS-20/600, Art 274 para 4 lit h and j DelVO 2015/35, margin no. 37 lit h and m EIOPA-BoS-20-002 and Art 30 para 3 lit e sublit i) to iv) and Art 28 para 6 DORA Regulation. It also implements Art 8 (2) DelVO (EU) 2024/1773 (RTS on testing).

[15] See Art 274 para 4 lit f DelVO 2015/35.

[16] See Art 274 para 4 lit i DelVO 2015/35.

[17] See Art 274 para 4 lit f DelVO 2015/35.

[18] This point implements Art 30 para 2 lit g DORA Regulation.

[19] This point implements Art 30 para 3 lit d DORA Regulation.

[20] See also margin no. 37 lit j EIOPA-BoS-20-002.

This point implements, among other things, Art 8 para 2 lit d DelVO (EU) 2024/1773 (RTS specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers).

[21] This chapter implements margin no. 37 b of EIOPA-BoS-20-002, Art 274 (4) lit d DelVO 2015/35 and Art 30 (2) lit h and Art 28 (7) DORA Regulation.

[22] This point implements Art 28 (7) DORA Regulation.

[23] This point implements Art 7 (1) RTS on subcontracting.

[24] This point implements Art 30 (2) (a) DORA Regulation and R 37 (a) EIOPA Guidelines EIOPA-BoS-20-002.