Non-binding model clauses for contracts on information and communication services

Note: The following non-binding model clauses are not a complete ICT contract. Rather, the non-binding model clauses represent an orientation by the association for the drafting of individual important regulatory components of an ICT contract. The model clauses have not been approved by the supervisory authorities. The association assumes no guarantee or liability for completeness and correctness.

DORA = Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Digital Operational Resilience Act)

RTS TPPol = Delegated Regulation (EU) 2024/1773; supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards 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

RTS-E SUB = Draft Regulatory Technical Standard 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 Article 30(5) of Regulation (EU) 2022/2554

ITS Register = Implementing Technical Standard (EU) 2024/2956 on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

Regulation content		**Non-binding model formulation**	**Information / Interaction Outsourcing**
DORA Level 1	RTS Level 2		
Chapter 1 – Preliminary notes			
Preliminary note **[Optional]***		**[Optional]** The Contractor is aware that the Client is subject to insurance supervisory requirements. In particular, these include the requirements of the German Act on the Supervision of Insurance Undertakings ('VAG'), the Minimum Requirements on the System of Governance of Insurance Undertakings ('MaGo'), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ('DORA'), Directive 2009/138/EC of the European	-

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		Parliament and of the Council of Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) and the legal acts adopted by the European Insurance and Occupational Pensions Authority ('EIOPA') and the German Federal Financial Supervisory Authority ('BaFin'). This framework agreement and the individual agreements concluded on its basis **[delete as appropriate/adapt individually]** must observe and comply with the above requirements - insofar as relevant within the scope of the present performance obligations.	
Preliminary note **[Optional]**		**[Optional]** The Contractor guarantees to provide the contractual services in full compliance with all legal, regulatory and official provisions and relevant case law that are applicable to the Client and are part of the Contractor's direct scope of services, in particular in accordance with Sections 23 et seq. VAG, the MaGo, Art. 274 of Regulation (EU) 2015/35 and DORA, including the specific delegated acts and implementing acts as amended from time to time and all relevant provisions and interpretative decisions of BaFin, EIOPA or their legal successors or other competent supervisory authorities (these requirements collectively 'Legal Provisions') **[to be adapted/added on a company-specific basis if necessary]**. The contracting parties shall support each other in complying with all Legal Provisions.	-

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		The contracting parties agree that the contracting of contractual services to the Contractor shall not impair the Client's ability to comply with the Legal Provisions. The Contractor shall enable the Client to monitor and assess the performance of the services on an ongoing basis so that any necessary corrective action can be taken immediately.	
Chapter 2 – Minimum requirements for all ICT contracts			
Art. 30 para. 1 The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format.		**[to be completed individually]**	In addition to the listed contractual requirements, other topics not explicitly mentioned in the catalogue of Art. 30 para. 2 DORA may need to be contractually regulated, for example with regard to additional information obligations.
Art. 30(2)(a) a clear and complete description of all functions and ICT services to be provided by the third-party ICT service provider, indicating whether subcontracting of an ICT		The Contractor shall provide the Client with the service(s) including service levels (including updates and revisions) specified in detail [in the contract / in the annex or service certificate/SLA] from/on the date/period specified [in the contract / in the annex or service certificate/SLA].	It may be advisable to assign the specific service to one of the ICT service types listed in the ITS on the Register of information in the contract/SLA.

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

service supporting a critical or important function, or material parts thereof is permitted and, when that is the case, the conditions applying to such subcontracting.		**[With regard to the subcontracting of services supporting critical/important functions, please refer to Chapter IV. Otherwise to be completed on a company-specific or service-specific basis]**	
Art. 30(2)(b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT thirdparty service provider to notify the financial entity in advance if it envisages changing such locations;		[**Individual contract level**] The performance of the services and the processing of the data, including storage, shall be carried out by the Contractor and, if applicable, its subcontractors exclusively at the locations (regions and/or countries) listed in [Annex X]. The Client shall be informed in advance [specification of time period] at least in text form if the contractor or its subcontractor intends to change these locations.	The contracting parties may consider an objection solution in the event of an intended change from EU or EEA to non-EU or non-EEA storage locations. If this leads to a significant change in the risk analysis, a right of cancellation makes sense.
Art. 30(2)(c) provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;		The Contractor is obliged to ensure the protection of the Client's data [**to be specified in detail if necessary**] when performing the contractual services. [**Reference to processing agreement if applicable**] The Contractor shall comply with all relevant laws and regulations on the protection of personal data when providing the contractually owed services [**refer to processing agreement/TOMs/C2C-TOMs if applicable**]. In order to ensure state-of-the-art	Note: Information may also be relevant for the register of information.

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		protection of the availability, integrity, authenticity and confidentiality of the other Client Data, the Contractor shall implement the measures described in **[Annex X (TOMs)]** accordingly and maintain them during the term of the contract. The Contractor shall continuously review these measures and adapt them as necessary in order to ensure state-of-the-art protection. When using systems, components and processes that are not subject to its access, the Contractor shall impose corresponding obligations on its contractual partners and regularly monitor compliance with these obligations. This also includes the obligation to disclose information to the client which the client requires for a necessary risk analysis.	
Art. 30(2)(d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;		In the event of insolvency, liquidation, cessation of the Contractor's business activities or termination of the contractual agreement, the Contractor shall remain obliged **[under the contractual conditions]** to grant access to personal and non-personal data until such time as this data has been recovered or returned **[at the Client's choice deletion instead of return] [but for no longer than X months].** The return must be made on request in an easily accessible, customary format **[specified by the Client]** to the Client or to a third party named by the Client. **[Alternatively: The Contractor warrants that in one of the above cases the Client can export the data independently or with the support of the Contractor. The complete export shall be made**	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		available to the Client within a maximum of XX working days. A right of retention cannot be asserted against the request to export the data]. After successful return [or as an alternative to return], the Contractor shall irrevocably delete any remaining databases of the Client in accordance with the current state of the art and provide proof of this at the request of the Client. **[This shall not apply if and as long as the Contractor can invoke a legal reason for the continued storage.]** [**Optional**] If there is a possibility that the Client's ability to access its data at the Contractor is threatened or could foreseeably be threatened by third-party measures (such as seizure or confiscation), by insolvency or composition proceedings or by other events, the Contractor shall inform the Client immediately and shall do everything necessary on its part to ensure the Client's ability to access the data. In this context, the Contractor shall immediately inform all responsible bodies and parties involved that the (decision-making) sovereignty over the data lies exclusively with the Client.	
Art. 30 (2)(e) service level descriptions, including updates and revisions thereof;		**[To be added on a company or service-specific basis]**	
Art. 30 (2) (f) the obligation of the ICT third-party service provider to provide assistance to the financial		The Contractor is obliged to provide support to the Client in the event of an ICT incident related to the ICT service provided to the Client.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs;		The Contractor shall provide the support services without additional remuneration / at the following conditions [**delete as appropriate and adapt individually**]	
Art. 30 para. 2 lit. g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;		The Contractor agrees to fully cooperate with the competent authorities of the Client, in particular also with the supervisory and resolution authorities, including other persons appointed by them.	
Art. 30 para. 2 lit. h) termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities; Art. 28 (7) Art. 31 para. 12		The Client [**both parties**] shall have the right to extraordinary termination for good cause. The parties agree that the client is entitled to extraordinary termination for good cause in particular in the following circumstances: a) a significant breach by the Contractor [and/or its subcontractors] of applicable laws, regulations or conditions of this Contract; b) circumstances identified in the course of ICT third party risk management within the meaning of Art. 3 No. 18 of Regulation (EU) 2022/2554 which are assessed as likely to affect the performance of the functions and ICT services provided under the contractual agreement, including material changes affecting the	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		agreement or the Contractor's circumstances (e.g. change of control); c) demonstrable weaknesses of the Contractor in relation to its general ICT risk management and in particular in the manner in which it ensures the availability, authenticity, security and confidentiality of data, whether personal or otherwise sensitive data or non-personal data; d) the competent authority can no longer effectively supervise the client [or its client/the financial company] as a result of the terms of the relevant contractual arrangement or the circumstances relating to that arrangement. For the avoidance of doubt, this circumstance only exists if the authority demands termination of the contractual agreement or an amendment on which the parties cannot agree; e) The Contractor's financial circumstances deteriorate significantly and the Client cannot reasonably be expected to adhere to this contract; f) The contractor is established outside the EU, has been designated as critical within the meaning of Article 31(1)(a) of Regulation (EU) 2022/2554 and has no subsidiary in the Union nor intends to establish one within 12 months of being designated as critical; g) other circumstances that would lead to an unacceptable increase in risk from the perspective of the Client.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		[Termination periods to be supplemented on a company-specific basis]	
Article 30(2)(i) the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6).		**[The conditions are to be customised for each company individually]** Both parties guarantee each other that they will sensitise their personnel involved in the service provision to the required extent with regard to ICT security and keep their knowledge up to date through training to the required extent. To this end, the Client shall offer programmes to raise awareness of ICT security and training on digital operational resilience (collectively: ICT qualification). At the request of the Client, the Contractor shall instruct the personnel it deploys to provide the contractually owed services to participate in an ICT qualification programme of the Client [**add external providers if applicable**]. The Contractor may only reject a request if it can prove that the personnel deployed have participated in an ICT qualification with comparable content in the past **XX** months. The parties shall agree on details of the scope and implementation of the ICT qualification within **XX** weeks of the request.	Consistency with internal training requirements should be ensured. If necessary, regulations on any reimbursement of costs in connection with the training (such as travel expenses) may be useful.
Incidents reports		The Contractor shall report ICT-related incidents within the meaning of Art. 3 No. 8 DORA to the Client insofar as these may have an impact on the ICT service owed. It shall also report significant cyber threats within the meaning of Art. 3 No. 13 DORA if these could jeopardise the ICT service owed. The notification	Annex **X** may also regulate pre-classification by the service provider.

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		period, content of the specific notification and the notification procedure were agreed between the parties on the basis of the process pursuant to Art. 17 DORA and documented in **Annex X**.	
Chapter 3 - Additional requirements for the support of critical/important functions or material parts of it			
	Art. 8 para. 4 RTS TPPol		Material changes to the contractual agreement are formalised in a written document, dated and signed by all parties, which specifies the procedure for renewing the contractual agreement.
Art. 30(3) The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least the following a) full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative	Art. 9 para. 1 and 2 RTS TPPol	The Contractor shall provide the Client with the service(s) specified in detail [in the contract / in the annex to the contract or in the service level agreement (SLA)] in the service quality described therein (service level), compliance with which is guaranteed by the agreement of quantitative and qualitative performance targets. The Contractor shall grant the Client the right to monitor the Contractor's performance on an ongoing basis in order to enable appropriate corrective measures to be taken immediately to restore the agreed service level if this is not achieved. To enable ongoing monitoring of the agreed performance targets, the Contractor shall be obliged to	In the case of outsourcing of important functions and insurance activities, consider right to issue instructions (Art. 274 para. 4 lit. f) Regulation (EU) 2015/35)

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;		draw up and send a report to the Client. The form and interval of the reporting are regulated **[in Annex X]**. Updates or revisions of the service level shall be agreed by means of a corresponding amendment [in the contract / in the annex to the contract or in the service level agreement (SLA)] **[if necessary, add company-specific measures and key indicators for monitoring performance]** [Optional] Both contracting parties shall each appoint a responsible contact person for the contractual and administrative coordination. The contracting parties shall consult with each other on a regular basis regarding the quality of service provision, problem cases and upcoming changes to the scope of services (updates and revisions). Both contracting parties are obliged to participate in those meetings.	
	Art. 9 para. 1 RTS TPPol	**[if necessary, contractually agree company-specific consequences if the agreed service level is not achieved]**	Can already be added to the service level clause above if necessary
Art. 30(3)(b) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on	Art. 9 para. 2 RTS TPPol	The Contractor shall regularly provide the Client with appropriate reports on its activities and services, as well as reports on incidents, including operational or security incidents related to payments, ICT security and business continuity measures and tests. In particular, the Contractor shall promptly report to the Client any developments that could have a material impact on its ability to effectively provide ICT services in accordance with the agreed service levels, including	Alternatively, a standardised clause - consisting of the reporting obligations in the previous clause and this clause - may be selected for ongoing monitoring, for example: *"To enable ongoing monitoring of service level against the agreed performance targets and to enable risk management, the*

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;		ICT-related incidents and operational or security incidents related to payments. [**Cancellation periods or termination terms to be completed individually in accordance with Article 10 RTS TPPol**]	*Contractor shall draw up and submit reports to the Client (e.g. reports on incidents, on the provision of services, on ICT security and on business continuity measures and tests). In particular, the Contractor shall immediately notify the Client of any developments that could have a significant impact on its ability to provide ICT services in accordance with the agreed arrangements, including ICT-related incidents and operational or security-related incidents in connection with payments. The form, content, addressees and interval of the reporting are regulated [in Annex **X**]."*
Art. 30(3)(c) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services		The contractor implements and tests business contingency plans and has measures, tools and guidelines for ICT security that provide an appropriate level of security for the provision of services by the client in accordance with its legal framework. **[to be specified on a company or service-specific basis where applicable]**	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

by the financial entity in line with its regulatory framework;			
Article 30(3)(d) the obligation of the ICT third-party service provider to participate and fully cooperate with the financial company's TLPTs referred to in Articles 26 and 27;		The Contractor is obliged to participate and fully co-operate in the Client's threat-led penetration testing (TLPT) in accordance with Regulation (EU) 2022/2554 (DORA). Competent authorities shall identify financial companies to carry out TLPTs taking into account the criteria set out in Article 4(2) of the DORA Regulation. **[Optional]** The following regulations apply to the performance of threat-led penetration tests: (a) they shall normally take place at least every three (3) years, unless legal requirements applicable to the Client or orders by competent authorities prescribe otherwise; b) The Contractor shall apply effective risk management controls to mitigate the risk of potential impact on data, damage to assets and disruption of critical or important functions, services or operations; c) The Contractor shall take reasonable steps to ensure compliance with the **[SLA]** in relation to the availability, authenticity, integrity and confidentiality of third party data, including the protection of personal data; d) The client and the appointed testers will make pictures and/or copies of the data and information that come to their attention for documentation purposes; e) **[reference to confidentiality where applicable]**	It may be useful to regulate what happens if data is lost during a live attack

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		The following requirements apply to the appointed testers for threat-orientated penetration tests: (a) They shall be of the highest suitability and reputation; b) They possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing c) They are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks; d) They provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and redress for the business risks of the financial entity; e) They are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence	
Art. 26(4)		**[Optional]** The Contractor is allowed to conclude contractual arrangements with an external tester to conduct a pooled threat-led penetration test under the direction of a financial company which is subject to Regulation (EU) 2022/2554 and is designated by the Contractor, involving several financial companies subject to Regulation (EU) 2022/2554 for which the Contractor provides services ('Pooled Test'), if it can reasonably be assumed, a) that the threat-led penetration test will adversely affect the quality or security of services provided by the Contractor to other entities falling out of the scope of Regulation (EU) 2022/2554; or b) that the threat-led penetration test adversely affects the confidentiality of the data associated with these services.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		When performing pooled tests, the Contractor shall structure the contractual agreements with the external tester in such a way that the Client can comply with the regulatory and data protection requirements and the corresponding agreements are in accordance with this Framework Agreement and/or the individual agreements and/or the Annexes, in particular the content and scope of Annex **X**.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

Art. 30 para. 3 lit. e) the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following: i) unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies; ii) the right to agree on alternative assurance levels if other clients' rights are affected; iii)	Art. 3 para. 8 and Art. 8 para. 2 and 3 lit. c and g; Art. 9 para. 1 RTS TPPol	The Client shall have the right to monitor the Contractor's performance on an ongoing basis. This includes in particular: a) The client has the right to ICT testing and effective access to premises and information related to the ICT service provided. b) The client, including its central outsourcing management, internal audit, data protection officer, compliance officer, a third party appointed by the client or competent authorities, auditors and the competent authorities have unrestricted access, inspection and audit rights, including pooled audits, as well as the right to make copies of relevant documents on site if they are critical to the operations of the ICT third-party service provider. Agreements, implementation guidelines or internal specifications of the Contractor that hinder or restrict the actual exercise of these rights shall be ineffective. c) The client has the right to assure itself in a manner other than via the agreed access, inspection and audit rights that the agreements made with the contractor are complied with if the rights of other clients are affected (alternative level of confirmation). d) The Contractor agrees to cooperate fully with the competent authorities, in particular during on-site inspections and audits carried out by the competent authorities, the lead overseer, the Client or an appointed third party.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits; See also Article 28(6) (predetermination of the frequency of audits and inspections)		e) With regard to the scope and frequency of inspections and audits and the procedure to be followed, the parties agree on the following: **[based on the results of Art. 28 Para. 6; if applicable, Annex - to be supplemented individually]** f) **[If third-party certifications or external audits shall be used]:** The client has the right to request changes to the scope of the certifications or audit reports with regard to other relevant systems and controls at a risk-based frequency. In addition, it has the right to carry out individual and pooled audits with regards to the contractual arrangements **X** times a year at its own discretion. **g) [The specific measures and key indicators for monitoring the service provider's performance, including measures to monitor the confidentiality, availability, integrity and authenticity of data and information and the service provider's compliance with Clients relevant policies and procedures, shall be contractually defined].** **[add company-specific if necessary]**	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

Art. 30 para. 3 lit. f) exit strategies, in particular the establishment of a mandatory adequate transition period			It may be useful to refer to an annex regarding specific framework parameters for the exit.
i) during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;		In the event of full or partial termination of the contract by one of the contracting parties, whether by cancellation or withdrawal, the Contractor shall continue to provide the services under the contractual conditions, in particular with regard to compliance with regulatory requirements and the continuity and quality of the services, for up to **XX** months following a unilateral declaration by the client.	Note: May not be sufficient to ensure a smooth transition without further details.
ii) allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.		In the event of full or partial termination of the contract by one of the contracting parties, whether by cancellation or withdrawal, the Contractor shall also facilitate the transfer of the agreed services to another company or back to the Client. The Contractor shall support the Client in avoiding interruptions, disruptions or other impairments to the Client's business operations when transferring the services to another company or back to the client.	
By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access, inspection and audit can be delegated to an			

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.			
Chapter 4 - Conditions for subcontracting when supporting critical/important functions or material parts thereof			
Art. 30 para. 2 lit. a		**Consent variant** The Contractor may subcontract all or part of the service by written contract (text form is sufficient) (external procurement or subcontracting) if it notifies the Client of this in advance in writing (text form is sufficient) **[at least XX weeks if necessary - the period is to be determined individually]** and the Client then agrees in writing (text form is sufficient). **[Optional]:** The client must be informed prior to the execution of subcontracting of third parties approved in writing. The Client is aware that the Contractor has currently already engaged [name/address of the subcontractor(s) and activity performed - or reference to a corresponding contractual annex] in the aforementioned sense.	Note: The conditions and decision on subcontracting are basically free within the general regulatory requirements and specifications of DORA and the RTS-E SUB. In order to provide initial guidance, this chapter is preceded by formulations for the 'consent' variants (including the optional additional 'withdrawal of consent' option) and an 'objection solution'. These options are not exhaustive. A more detailed wording, including individual components of the following requirements from the draft RTS on subcontracting, can be found at the end of this chapter.

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		[Optional] Revocation of consent Even after consent has been given, the client has the right to revoke it for good cause at any time. Good cause shall be deemed to exist in particular if a. there is reasonable cause to doubt that the subcontractor will perform the agreed service properly, b. the assertion of the aforementioned rights is not ensured, c. the competent supervisory authority objects to the subcontracting, d. the subcontractor relocates its registered office outside the [EU/EEA] or customer-related data processing outside the [EU/EEA], e. the subcontracting of a service affects the effectiveness of the client's supervision of this service in any way, f. the subcontractor does not have sufficient resources, abilities, and experience to perform the respective tasks, or g. the competent supervisory authority can no longer supervise that the client fulfils its legal obligations.	Cancellation as a milder means before - otherwise still possible - termination.
		Objection Variant The Contractor shall only be entitled to subcontract (external procurement or subcontracting) all or parts of the service by written contract (text form is sufficient) if the Client does not object to such subcontracting within **[XX weeks - the period is to be determined individually depending on the company]** after being fully informed of the planned subcontracting.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

	Art. 4a and b RTS-E SUB	The Contractor is obliged to monitor all subcontracted ICT services related to the ICT service provided to the Client to ensure that its contractual obligations to the Client are continuously met. It shall remain responsible to the Client for the provision of the agreed services by subcontractors.	
	Art. 4c RTS-E SUB	If weaknesses, deficiencies, or incidents are identified at the subcontractor during the monitoring process, the Contractor shall inform the Client of this immediately by submitting the results in text form.	To be read in conjunction with the previous clause (on Art. 4a and b RTS-E SUB).
	Art. 4d RTS-E SUB	Prior to subcontracting and continuously, the Contractor shall assess all subcontracting risks, including ICT risks, arising from the location of the subcontractor, its parent company and the location where the service is provided from in the specific case. The results of this assessment must be submitted to the client.	The level of detail and interval may vary depending on the service provider and supported function
	Art. 4e RTS-E SUB	**[If applicable]**	Note: the clause on Art. 30 para. 2 lit. b) may already cover this
	Art. 4f RTS-E SUB	In relation to the subcontractor, the Contractor must specify the monitoring and reporting obligations towards the Contractor **[and, if applicable, the Client]** in a written agreement. These must be appropriate to the risk of subcontracting and designed in such a way that the contractor can fulfil its monitoring and reporting obligations to the client.	
	Art. 4g RTS-E SUB	The Contractor shall ensure that the service to be provided for the Client can be provided continuously throughout the entire subcontractor chain even if the subcontractor fails to meet its contractually agreed service level. In the written agreement between the Contractor and the subcontractor, the implementation and testing of business contingency plans shall be agreed and the respective service level in relation to these plans shall be defined. The Contractor shall ensure that the business contingency plans harmonise	Emergency plans are the subject of Art. 30 para. 3 lit. c - harmonisation may be necessary

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		with those agreed between the Client and the Contractor.	
	Art. 4h RTS-E SUB	The Contractor shall ensure in a written agreement that the subcontractor has measures, tools and guidelines for ICT security that provide an appropriate level of security for the provision of services by the Client in accordance with its legal framework.	Note: Security standards are the subject of Art. 30 para. 3 lit. c - harmonisation may be required.
	Art. 4i RTS-E SUB	The Contractor shall ensure that the Client, its supervisory and resolution authority, and persons appointed by them have direct audit, access and inspection rights vis-à-vis the subcontractor at least to the same extent as those agreed between the Client and the Contractor.	
	Art. 4k RTS-E SUB	Without prejudice to further rights of termination, the client shall be entitled to terminate the contract in the following cases: a) the provided service does not achieve the service level agreed with the client b) the Contractor subcontracts or makes significant changes to the subcontracting despite rejection and request for change or lack of consent **(delete as appropriate)** of the Client or before the review period expires without consent. c) **[optional]** The Contractor continues to subcontract a service despite the revocation of consent. d) The contractor engages a subcontractor for a service that supports an important or critical function for which the contractual agreement does not provide an explicit subcontracting option. e) The contractor engages a subcontractor for a service that supports an important or critical function for which a prohibition on subcontracting has been contractually agreed.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		f) The contractor breaches the conditions of subcontracting in a significant manner.	
	Art. 5 para. 1, 2, 3 and 4 RTS-E SUB	The Contractor is obliged to provide the Client with all information required to monitor the entire contract chain for assessment and documentation at the Client's premises. The Contractor shall agree the corresponding obligations in contracts with subcontractors. In addition to quantitative and qualitative performance indicators and the service provider reports in accordance with **Chapter XX (clause to Art. 30 Para. 3 lit. b DORA**) of the subcontractors for the assigned contract, this also includes the submission of the relevant contractual agreements between the contractor and subcontractors as well as between other subcontractors insofar as they relate to the specific service. In particular, this concerns all information relating to the contract chain that is to be filled into the register of information pursuant to Art. 28 (3) of Regulation (EU) 2022/2554, specified by the Regulation (RTS-E SUB and ITS Register) or that is required for an assessment of the impact of the complexity or length of the subcontracting chain on the ability of effective monitoring by the Client or the competent supervisory authorities. For this purpose, the information must be kept up to date.	Note: The client can provide the contractor with a questionnaire to be filled out for this purpose.
	Art. 4 para. 1 lit. j; 6 para. 1 and 2 RTS-E SUB	If the Contractor intends to make significant changes to subcontracting arrangements, including the initial or further engagement of subcontractors, it must inform the Client **XX** weeks in advance. The Client shall assess the impact of the planned changes on the risk analysis and inform the Contractor of the result.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

	Art. 6 Abs. 2 RTS-E SUB	The Contractor may only implement the changes if the Client has approved the changes or has not objected to them by the end of **XX** weeks after notification of the planned change. If further information is required for a risk assessment, the expiry of the deadline is suspended for the period until the information is provided. Following this, the client must have at least **XX** weeks to evaluate the subsequently provided information.	In conjunction with the previous standard clause.
	Art. 6 para. 3 RTS-E SUB	The client has the right to demand modifications to the planned change of subcontracting before its implementation if the risk analysis shows that the planned change exceeds the client's risk appetite. It shall inform the Contractor of the result of the risk analysis. If the Client and Contractor are unable to reach an amicable solution in this case, the Client shall have a special right of termination.	
	Art. 3 para. 1 lit. c RTS-E SUB	The Contractor shall agree to reproduce the essential contractual provisions concluded with the Client in this contract in the contracts with subcontractors in such a way that the Client is able at all times to continuously comply with its legal and regulatory obligations, in particular those arising from Regulation (EU) 2022/2554. It shall grant the same contractual audit, access and inspection rights along the chain of subcontractors providing ICT services supporting critical or important functions to the client, its supervisory and resolution authority and third parties appointed by them as the contractor grants in relation to the Client. **[to be individually added if necessary, for example: In addition to the appropriate level of cybersecurity, this relates in particular to the inspection, cooperation and information obligations of the client or towards the client, etc.].**	Note: further restrictions may be possible in individual cases.

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

Elements of (preliminary) due diligence, which could also be contractually agreed as an option			
	Art. 3 para. 1 lit. a, d RTS-E SUB	**[optional]** The Contractor shall disclose and explain to the Client the details of the due diligence process for subcontractors and the involvement in operational reporting and testing obligations.	
	Art. 3 para. 1 lit. f RTS-E SUB	**[optional]** The Contractor shall support the Client in analysing the impact of a potential failure of the subcontractor on the digital operational resilience and financial soundness of the Client. To this end, the Contractor shall disclose the necessary information to the Client.	
	Art. 3 para. 2 RTS-E SUB	**[optional]** The Client shall regularly review the risk assessment for the use of subcontractors for changes, in particular with regard to the supported function, ICT threats, concentration risks and geopolitical risks. The Contractor shall be obliged to provide the Client with the necessary information for this purpose.	
More detailed formulation of the introductory clause with partial inclusion of further sample clauses			
		[Alt. 1: Consent regulation for ICT services to support critical or important functions]: The Contractor may only subcontract (external procurement or sub-outsourcing) all or part of the service if the Client has consented to this sub-delegation in written form (text form is sufficient). The Contractor shall notify the Client of the planned sub-delegation in writing (text form is sufficient) in advance [at least XX weeks if necessary - the period is to be determined individually], stating the suitability and reliability of the third party and providing a precise description of the sub-contracted activities. The Contractor shall provide	Note: The more detailed wording “consent variant” already contains elements from: - Art. 30 para. 2 lit. a DORA - Art. 5 para. 1 RTS-E SUB - Art. 5 para. 2 RTS-E SUB - Art. 6 para. 4 RTS-E SUB - Art. 4 lit. h RTS-E SUB - Art. 4 lit I RTS-E SUB - Art. 4 lit. c RTS-E SUB - Art. 4 lit. g RTS-E SUB - Art. 3 lit. f RTS-E SUB

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		all information required for a risk analysis at the Client. For this purpose, the Client may provide the Contractor with a questionnaire. The Client shall have the right to request changes to the proposed subcontracting changes prior to their implementation if the risk assessment shows that the planned subcontracting or changes to the subcontracting by the Contractor expose the Client to risks within the meaning of Article 3(1) RTS-E SUB that exceed its risk appetite. If the Client gives its written consent (text form is sufficient), the Contractor ensures that the service is performed to the same standards and in the same quality as under this contract. In this respect, the Contractor and the subcontractor shall also conclude a written agreement (text form is sufficient). In particular, this shall ensure that the subcontractor must contractually fulfill the obligations of the contractor to the required extent and that the client, its internal auditors, compliance officers, data protection officers, central outsourcing management, a competent supervisory authority and third parties appointed by them (e.g. auditors) can directly assert their rights granted under this contract. In the event of subcontracting, the Contractor shall remain obliged to report to the Client. The Contractor shall remain responsible for the fulfilment of the subcontracted activities as if they were carried out by the Contractor itself. The Contractor shall disclose the contract with the subcontractor at the request of the Client. **[Optional]** The Client must be informed in a timely manner prior to the execution of a subcontracting of third parties that has been approved in writing. Even after	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		written consent has been granted, the Client has the right to revoke it at any time for good cause. Good cause shall be deemed to exist in particular if a) there is reasonable cause to doubt that the subcontractor will properly perform the agreed service, b) the assertion of the aforementioned rights is not ensured, c) the competent supervisory authority objects to the subcontracting, d) the subcontractor relocates its registered office outside the [EU/EEA] or customer-related data processing outside the [EU/EEA], e) the subcontracting of a service in any way impairs the effectiveness of the client's supervision of that service f) the subcontractor does not have sufficient resources, abilities, and experience to perform the service, or g) the competent supervisory authority can no longer supervise that the client fulfils its legal obligations.	
		[Alt. 2 Objection clause]: The Contractor shall only be authorized to subcontract (external procurement or subcontracting) the assumed service in whole or in part by written contract (text form is sufficient) if it is ensured that the assumed service is performed according to the same standards and in the same quality as under this contract. This requires in particular that the subcontractor must contractually fulfil the obligations of the contractor to the required extent and that the client, its internal audit department, compliance officer, data protection officer, central outsourcing management, or a competent supervisory authority as well as third parties appointed by them (e.g. auditors) can directly assert their rights granted under this contract. In the event of subcontracting, the	Note: The more detailed wording “objection variant” already contains elements from: - Art. 30 para. 2 lit. a DORA - Art. 5 para. 1 RTS-E SUB - Art. 5 para. 2 RTS-E SUB - Art. 6 para. 4 RTS-E SUB - Art. 4 lit. h RTS-E SUB - Art. 4 lit I RTS-E SUB - Art. 4 lit. c RTS-E SUB - Art. 4 lit. g RTS-E SUB - Art. 3 lit. f RTS-E SUB

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		Contractor shall remain obliged to report to the Client. The Contractor shall remain responsible for the fulfillment of the subcontracted services as if they were carried out by the Contractor itself. The Contractor shall disclose the contract with the subcontractor to the Client on request. The Client shall have the right to request changes to the proposed subcontracting changes prior to their implementation if the risk assessment shows that the planned subcontracting or changes to the subcontracting by the Contractor expose the Client to risks within the meaning of Article 3(1) RTS-E SUB that exceed its risk appetite. The Client shall be informed in written form with a notice period of **[if applicable, at least XX weeks - the period shall be determined individually depending on the company]** prior to the execution of a subcontracting, stating the suitability and reliability of the third party as well as a precise description of the services to be subcontracted. Upon request, the Contractor shall provide further information required by the Client for the risk assessment. For this purpose, the Client may provide the Contractor with a questionnaire. The client has the right to reject the subcontracting for good cause. Good cause includes, in particular, if a) there is reasonable cause to doubt that the subcontractor will perform the agreed service properly, b) the assertion of the aforementioned rights is not ensured, c) the competent supervisory authority objects to the subcontracting,	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.

		d) the subcontractor has its registered office outside the [EU/EEA] or customer-related data processing outside the [EU/EEA], e) the subcontracting of a service in any way impairs the effectiveness of the client's supervision of that service f) the subcontractor does not have sufficient resources, abilities, and experience to perform the service, or g) the competent supervisory authority can no longer supervise that the client fulfils its legal obligations.	
		[Alt. 3, if subcontractors have already been evaluated at the time of conclusion of the contract and are to be accepted]: The Client is aware that the Contractor has currently already engaged **[name/address of subcontractor(s) and activity performed - or reference to a corresponding contract annex**] in the aforementioned sense. **[Optional for approval variant]:** These are deemed to be approved.	

* Optional content or content that may need to be added individually is marked in brackets and highlighted in yellow.