Official Journal
of the European Union

EN
L series

2024/1773

25.6.2024

COMMISSION DELEGATED REGULATION (EU) 2024/1773

of 13 March 2024

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ([1]), and in particular Article 28(10), third subparagraph, thereof,

Whereas:

(1) The framework on digital operational resilience for the financial sector established by Regulation (EU) 2022/2554 requires that financial entities set out certain key principles to manage ICT third-party risk, which are of particular importance when financial entities engage with ICT third-party service providers to support their critical or important functions.

(2) Financial entities, as part of their ICT risk management framework, are to adopt, and regularly review, a strategy on ICT third-party risk. In accordance with Article 28(2) of Regulation (EU) 2022/2554, that strategy is to include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. It is to apply on an individual and, where relevant, on a sub-consolidated and consolidated basis.

(3) Financial entities vary widely in size, structure, and internal organisation and in the nature and complexity of their activities and operations. It is necessary to take into account that diversity while imposing certain fundamental regulatory requirements which are appropriate for all financial entities when developing the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions by ICT third-party providers ('the policy), and to ensure that those requirements are applied in a manner that is proportionate.

(4) Where financial entities belong to a group, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group should therefore ensure that the policy is applied in a consistent and coherent way within the group.

(5) When applying the policy, ICT intra-group service providers, including those fully or collectively owned by financial entities within the same institutional protection scheme, should be considered as ICT third-party services providers. The risks posed by ICT intra-group service providers may be different but the requirements applicable to them are the same under Regulation (EU) 2022/2554. In a similar way, the policy should apply to subcontractors that provide ICT services supporting critical or important functions or material parts thereof to ICT third-party service providers, where a chain of ICT third-party service providers exists.

(6) The ultimate responsibility of the management body in managing a financial entity's ICT risk is an overarching principle which is also applicable regarding the use of ICT third-party service providers. This responsibility should be further translated into the continuous engagement of the management body in the control and monitoring of ICT risk management, including in the adoption and review, at least once per year, of the policy.

([1]) OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) To ensure appropriate reporting to the management body, the policy should clearly specify and identify the internal responsibilities for the approval, management, control and documentation of contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers ('contractual arrangements'), including the ICT services provided under contractual arrangements referred to in Article 28(1), point (a), of Regulation (EU) 2022/2554.

(8) In order to take into account all possible risks that may arise when contracting ICT services supporting critical or important function, the structure of the policy should follow all the steps of the each main phase of the life cycle for contractual arrangements with third-party providers.

(9) To mitigate the risks identified, the policy should specify the planning of contractual arrangements, including the risk assessment, the due diligence, and the approval process for new or material changes to those contractual arrangements. In order to manage the risks that may arise before entering into a contractual arrangement with an ICT third-party service provider, the policy should specify an appropriate and proportionate process to select and assess the suitability of prospective ICT third-party service providers and require that the financial entity takes into account a non-exhaustive list of elements that the ICT third-party service providers should have in place. The list should include elements related to the business reputation of the service providers, their financial, human and technical resources, their information-security, their organisational structure, including risk management, and their internal controls.

(10) To ensure a sound risk management in the provision of ICT services supporting critical or important functions by ICT third-party service providers, the policy should contain information about the implementation, monitoring and management of the contractual arrangements, including at consolidated and sub-consolidated level, where applicable. This includes requirements for the contractual clauses on mutual obligations of the financial entities and the ICT third-party service providers, which should be set out in writing. In order to ensure an efficient supervision and foster resilience in case of changes in the business model or business environment, the policy should ensure the financial entities' or appointed third parties' and competent authorities' rights to inspections and access to information and should also further specify the exit strategies and termination processes.

(11) To the extent personal data are processed by ICT third-party service providers, this policy and any contractual arrangements are without prejudice to and should complement the obligations under Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]), such as to have a written contract in place describing the personal data processing, requirement to ensure security of personal data processing and setting out all other elements required under that regulation.

([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) The Joint Committee of the European Supervisory Authorities referred to in Article 54 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([3]), in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([4]) and in Article 54 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([5]) has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential costs and benefits of the proposed standards and requested advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010, the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010, and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010,

(13) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([6]) and delivered an opinion on 24 January 2024,

HAS ADOPTED THIS REGULATION:

Article 1

Overall risk profile and complexity

The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the 'policy') shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and elements of increased or reduced complexity of its services, activities and operations, including elements relating to:

(a) the type of ICT services included in the contractual arrangement on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the 'contractual arrangement') between the financial entity and the ICT third-party service provider;

(b) the location of the ICT third-party service provider or the location of its parent company;

(c) whether the ICT services supporting critical or important functions are provided by an ICT third-party service provider located within a Member State or in a third country, also considering the location from where the ICT services are provided and the location where the data is processed and stored;

(d) the nature of the data shared with the ICT third-party service provider;

(e) whether the ICT third-party service provider is part of the same group as the financial entity to which the services are provided;

([3]) Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(f) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a competent authority in a Member State or subject to the oversight framework under Chapter V, Section II, of Regulation (EU) 2022/2554, and the use of ICT third-party service providers that are not;

(g) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a supervisory authority in a third country, and the use of ICT third-party service providers that are not;

(h) whether the provision of ICT services supporting critical or important functions are concentrated to a single ICT third-party service provider or a small number of such service providers;

(i) the transferability of the ICT services supporting critical or important functions to another ICT third-party service provider, including as a result of technology specificities;

(j) the potential impact of disruptions in the provision of the ICT services supporting critical or important functions on the continuity of the financial entity's activities and on the availability of its services.

Article 2

Group application

Where this Regulation applies on a sub-consolidated or consolidated basis, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group shall ensure that the policy is implemented consistently in all financial entities that are part of the group and is adequate for the effective application of this Regulation at all relevant levels of the group.

Article 3

Governance arrangements

1. The management body shall review the policy at least once a year and update it where necessary. Changes made to the policy shall be implemented in a timely manner and as soon as it is possible within the relevant contractual arrangements. The financial entity shall document the planned timeline for the implementation.

2. The policy shall establish or refer to a methodology for determining which ICT services support critical or important functions. The policy shall also specify when this assessment is to be conducted and reviewed.

3. The policy shall clearly assign the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements and shall ensure that appropriate skills, experience and knowledge are maintained within the financial entity to effectively oversee the relevant contractual arrangements, including the ICT services provided under those arrangements.

4. Without prejudice to the final responsibility of the financial entity to effectively oversee relevant contractual arrangements, the policy shall require that the ICT third party service provider is assessed to have sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements regarding the ICT services supporting critical or important functions that are provided.

5. The policy shall clearly identify the role or member of senior management responsible for monitoring the relevant contractual arrangements. The policy shall specify how that role or member of senior management shall cooperate with the control functions, unless it is part of it, and shall set out the reporting lines to the management body, including the nature of the information to report and the documents to provide. It shall also set out the frequency of such reporting.

6. The policy shall ensure that the contractual arrangements are consistent with the following:

(a) the ICT risk management framework referred to in Article 6 of Regulation (EU) 2022/2554;

(b) the information security policy referred to in Article 9(4) of Regulation (EU) 2022/2554;

(c) the ICT business continuity policy referred to in Article 11 of Regulation (EU) 2022/2554;

(d) the requirements on incident reporting set out in Article 19 of Regulation (EU) 2022/2554.

7. The policy shall require that ICT services supporting critical or important functions provided by ICT third party service providers are subject to independent review and are included in the audit plan.

8. The policy shall explicitly specify that the contractual arrangements:

(a) do not relieve the financial entity and its management body of its regulatory obligations and its responsibilities to its clients;

(b) are not to prevent effective supervision of a financial entity and are not to contravene any supervisory restrictions on services and activities;

(c) are to require that the ICT third party service providers cooperate with the competent authorities;

(d) are to require that the financial entity, its auditors, and competent authorities have effective access to data and premises relating to the use of ICT services supporting critical or important functions.

Article 4

Main phases of the life cycle for the adoption and use of contractual arrangements

The policy shall specify the requirements, including the rules, the responsibilities and the processes, for each main phase of the lifecycle of the contractual arrangement, covering at least the following:

(a) the responsibilities of the management body, including its involvement, as appropriate, in the decision-making process on the use of ICT services supporting critical or important functions provided by ICT third-party service providers;

(b) the planning of contractual arrangements, including the risk assessment, the due diligence as set out in Articles 5 and 6 and the approval process regarding new or material changes to contractual arrangements as set out in Article 8(4);

(c) the involvement of business units, internal controls and other relevant units in respect of contractual arrangements;

(d) the implementation, monitoring and management of contractual arrangements as referred to in Articles 7, 8 and 9, including at consolidated and sub-consolidated level, where applicable;

(e) the documentation and record-keeping, taking into account the requirements with regard to the register of information laid down in Article 28(3) of Regulation (EU) 2022/2554;

(f) the exit strategies and termination processes as set out in Article 10.

Article 5

Ex-ante risk assessment

1. The policy shall require that the business needs of the financial entity are defined before a contractual arrangement is concluded.

2. The policy shall require that a risk assessment is conducted at financial entity level and, where applicable, at consolidated and sub-consolidated level before a contractual arrangement is concluded.

The risk assessment shall take into account all the relevant requirements laid down in Regulation (EU) 2022/2554 and applicable sectoral Union legislation. It shall consider, in particular, the impact of the provision of ICT services supporting critical or important functions by ICT third-party service providers on the financial entity and all the risks posed by the provision of those ICT services supporting critical or important functions by ICT third-party service providers, including the following:

(a) operational risks;

(b) legal risks;

(c) ICT risks;

(d) reputational risks;

(e) risks linked to the protection of confidential or personal data;

(f) risks linked to the availability of data;

(g) risks linked to the location where the data is processed and stored;

(h) risks linked to the location of the ICT third-party service provider;

(i) ICT concentration risks at entity level.

Article 6

Due diligence

1. The policy shall set out an appropriate and proportionate process for selecting and assessing the prospective ICT third-party service providers taking into account whether or not the ICT third party service provider is an intragroup ICT service provider, and shall require that the financial entity assesses, before entering into a contractual arrangement, whether the ICT third-party service provider:

(a) has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organisational structure, risk management and internal controls and, if applicable, the required authorisations or registrations to provide the ICT services supporting the critical or important function in a reliable and professional manner;

(b) has the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework;

(c) uses or intends to use ICT sub-contractors to perform the ICT services supporting critical or important functions or material parts thereof;

(d) is located, or processes or stores the data in a third country and, if this is the case, whether this practice affects the level of operational or reputational risks or the risk of being affected by restrictive measures, including embargos and sanctions, that may impact the ability of the ICT third-party service provider to provide the ICT services or the financial entity to receive those ICT services;

(e) consents to contractual arrangements that ensure that it is effectively possible to conduct audits at the ICT third-party service provider, including onsite, by the financial entity itself, appointed third parties, and competent authorities;

(f) acts in an ethical and socially responsible manner, respects human rights and children's rights, including the prohibition of child labour, respects applicable principles on environmental protection, and ensures appropriate working conditions.

2. The policy shall specify the required level of assurance concerning the effectiveness of ICT third-party service providers' risk management framework for the ICT services supporting critical or important functions to be provided by an ICT third-party service provider. The policy shall require that the due diligence process includes an assessment of the existence of risk mitigation and business continuity measures and of how their functioning within the ICT third-party service provider is ensured.

3. The policy shall determine the due diligence process for selecting and assessing the prospective ICT third-party service providers and shall indicate which of the following elements are to be used for the required level of assurance on the ICT third-party service provider's performance:

(a) audits or independent assessments performed by the financial entity itself or on its behalf;

(b) the use of independent audit reports made on request by the ICT third-party service provider;

(c) the use of audit reports made by the internal audit function of the ICT third-party service provider;

(d) the use of appropriate third-party certifications;

(e) the use of other relevant information available to the financial entity or other information provided by the ICT third-party service provider.

4. Financial entities shall ensure an appropriate level of assurance on the ICT third-party service provider's performance, taking into account the elements listed in paragraph 3, points (a) to (e). Where appropriate, more than one element listed in those points shall be used.

Article 7

Conflicts of interest

1. The policy shall specify the appropriate measures to identify, prevent and manage actual or potential conflicts of interest arising from the use of ICT third-party service providers that are to be taken before entering relevant contractual arrangements and shall provide for an ongoing monitoring of such conflicts of interest.

2. Where ICT services supporting critical or important functions are provided by ICT intra-group service providers, the policy shall specify that decisions on the conditions, including the financial conditions, for the ICT services are to be taken objectively.

Article 8

Contractual clauses

1. The policy shall specify that the relevant contractual arrangement are to be in written form and are to include all the elements referred to in Article 30(2) and (3) of Regulation (EU) 2022/2554. The policy shall also include elements regarding requirements referred to in Article 1(1), point (a), of Regulation (EU) 2022/2554, as well as other relevant Union and national law as appropriate.

2. The policy shall specify that the relevant contractual arrangements are to include the right for the financial entity to access information, to carry out inspections and audits, and to perform tests on ICT. For that purpose, the policy shall require that the financial entity uses the following methods, without prejudice to the ultimate responsibility of the financial entity:

(a) its own internal audit or an audit by an appointed third party;

(b) where appropriate, pooled audits and pooled ICT testing, including threat-led penetration testing, that are organised jointly with other contracting financial entities or firms that use ICT services of the same ICT third-party service provider and that are performed by those contracting financial entities or firms or by a third party appointed by them;

(c) where appropriate, third-party certifications;

(d) where appropriate, internal or third-party audit reports made available by the ICT third-party service provider.

3. The financial entity shall not over time rely solely on certifications referred to in paragraph 2, point (c), or audit reports referred to in point (d) of that paragraph. The policy shall only permit the use of the methods referred to in paragraph 2, points (c) and (d), where the financial entity:

(a) is satisfied with the audit plan of the ICT third-party service provider for the relevant contractual arrangements;

(b) ensures that the scope of the certifications or audit reports cover the systems and key controls identified by it and ensures compliance with relevant regulatory requirements;

(c) thoroughly assesses the content of the certifications or audit reports on an ongoing basis and verifies that the reports or certifications are not obsolete;

(d) ensures that key systems and controls are covered in future versions of the certification or audit report;

(e) is satisfied with the aptitude of the certifying or auditing party;

(f) is satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

(g) has the contractual right to request, with a frequency that is reasonable and legitimate from a risk management perspective, modifications of the scope of the certifications or audit reports to other relevant systems and controls;

(h) has the contractual right to perform individual and pooled audits at its discretion with regard to the contractual arrangements and execute those rights in line with the agreed frequency.

4. The policy shall ensure that material changes to the contractual agreement are to be formalised in a written document which is dated and signed by all parties and shall specify the renewal process for the contractual arrangements.

Article 9

Monitoring of the contractual arrangements

1. The policy shall require that the contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis, the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures. The policy shall also specify measures that apply when service level agreements are not met, including contractual penalties where appropriate.

2. The policy shall specify how the financial entity is to assess whether the ICT third-party service providers used for the ICT services supporting critical or important functions meet appropriate performance and quality standards in line with the contractual arrangement and the financial entity's own policies. The policy shall, in particular, ensure the following:

(a) that the ICT third-party service providers provide appropriate reports on their activities and services to the financial entity, including periodic reports, incidents reports, service delivery reports, reports on ICT security and reports on business continuity measures and testing;

(b) that the performance of ICT third-party service providers is assessed with key performance indicators, key control indicators, audits, self-certifications and independent reviews in line with the financial entity's ICT risk management framework;

(c) that the financial entity receives other relevant information from the ICT third-party service providers;

(d) that the financial entity is notified, where appropriate, of ICT-related incidents and operational or security payment-related incidents;

(e) that an independent review and audits verifying compliance with legal and regulatory requirements and policies are performed.

3. The policy shall specify that the assessment referred to in paragraph 2 is to be documented and its results to be used to update the financial entity's risk assessment referred to in Article 6.

4. The policy shall establish the appropriate measures that the financial entity is to adopt if it identifies shortcomings of the ICT third-party service providers, including ICT-related incidents and operational or security payment related incidents, in the provision of the ICT services supporting critical or important functions or in the compliance with contractual arrangements or legal requirements. It shall also specify how the implementation of such measures is to be monitored in order to ensure that they are effectively complied with within a defined timeframe, taking into account the materiality of the shortcomings.

Article 10

Exit from and termination of the contractual arrangements

The policy shall contain requirements for a documented exit plan for each contractual arrangement and for the periodic review and testing of the documented exit plan. When establishing the exit plan, the following shall be taken into account:

(a) unforeseen and persistent service interruptions;

(b) inappropriate or failed service delivery;

(c) the unexpected termination of the contractual arrangement.

The exit plan shall be realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the contractual arrangements.

Article 11

Entry into force

This Regulation shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 13 March 2024.

For the Commission
The President
Ursula VON DER LEYEN