Official Journal
of the European Union

EN
L series

2025/532

2.7.2025

COMMISSION DELEGATED REGULATION (EU) 2025/532

of 24 March 2025

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the elements that a financial entity has to determine and assess when subcontracting ICT services supporting critical or important functions

(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 30(5), fourth subparagraph, thereof,

Whereas:

(1) The provision of ICT services to financial entities often depends on a complex chain of ICT subcontractors, whereby ICT third-party service providers may enter into one or more subcontracting arrangements with other ICT third-party service providers. Indirect reliance on ICT subcontractors may have an impact on a financial entity' ability to identify, assess, and manage its risks, including risks that are related to gaps in the information provided by ICT third-party service providers, and to the limited ability of a financial entity to obtain information from those ICT subcontractors that provide ICT services that support critical or important functions or material parts thereof. In that regard, where the provision of ICT services to financial entities depends on a potentially long or complex chain of ICT subcontractors, it is essential that financial entities identify the overall chain of subcontractors providing ICT services supporting critical or important functions.

(2) Among those subcontractors that provide ICT services that support critical or important functions, financial entities should focus in particular and continuously on those subcontractors that effectively underpin the ICT service that supports critical or important functions, including all the subcontractors that provide ICT services the disruption of which would impair the security or continuity of the service as laid down in the register of information referred to in Article 28(3) of Regulation (EU) 2022/2554.

(3) Financial entities vary widely in size, structure, internal organisation, and in the nature and complexity of their activities. To ensure proportionality, that diversity should be taken into account when specifying which elements a financial entity should determine and assess when subcontracting ICT services that support critical or important functions.

(4) When permitted by the financial entities in accordance with Article 30(2) of Regulation (EU) 2022/2554, the use of subcontracted ICT services supporting critical or important functions by ICT third-party services providers cannot reduce the ultimate responsibility for the management bodies of the financial entities to manage their risks and to comply with their legislative and regulatory obligations. Where subcontracting ICT services supporting critical or important functions is permitted, it is important that financial entities have a clear and holistic view of the risks associated with subcontracting services that support critical or important functions so that they are able to monitor, manage and mitigate those risks. They should therefore assess those risks before subcontracting those services.

(5) ICT intra-group subcontractors that provide ICT services that support critical or important functions or material parts thereof, including ICT intra-group subcontractors that are fully or collectively owned by financial entities within the same institutional protection scheme, should be considered as ICT subcontractors.

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

(6) Where applicable, in a group context, the parent undertaking of financial entities should ensure that the policy on the use of ICT subcontractors providing ICT services that support critical or important functions or a material part thereof is applied in a consistent and coherent way within the group.

(7) It is important to ensure a comprehensive management of the risks that can arise when ICT services that support critical or important functions are subcontracted. For that reason, financial entities should follow the steps of the life cycle of a contractual arrangement for the use of ICT services that support those functions and that are provided by ICT third-party service providers, including for subcontracting arrangements. It is therefore necessary to lay down requirements for financial entities that should be reflected in their contractual arrangements with ICT third-party service providers where the use of subcontracted ICT services supporting critical or important functions is permitted.

(8) To mitigate risks that are linked to subcontracting, it is necessary to specify the conditions under which ICT third-party service providers can use subcontractors for the provision of ICT services that support critical or important functions. For that purpose, ICT contractual arrangements between financial entities and ICT third-party service providers should set out such conditions, including the planning of subcontracting arrangements, the risk assessments, the due diligence, and the approval process for new ICT subcontracting arrangements on ICT services supporting critical or important functions or material parts thereof, or material changes to existing ones made by the ICT third-party service provider.

(9) To identify risks that could arise before a financial entity enters into an arrangement with an ICT subcontractor, ICT third-party service providers should assess, in appropriate and proportional way, the suitability of potential subcontractors on the basis of the ICT contractual arrangements that the ICT third-party service provider concluded with the financial entity. Those ICT contractual arrangements should therefore require the ICT third-party service provider, or the financial entity directly, as appropriate, assesses the resources of the potential subcontractor, including its expertise and whether it has the proper financial, human and technical resources, its information security, and its organisational structure, including the risk management and internal controls that the subcontractor should have in place.

(10) To mitigate any vulnerabilities and threats that may pose risks to their ICT systems and operations, financial entities should be able to monitor the performance of the ICT service and to be informed of any relevant changes within their ICT subcontracting chain where such changes concern critical or important functions.

(11) To enable financial entities to assess the risks associated with subcontracting arrangements or material changes thereto, ICT third-party service providers should inform the financial entities to which they provide ICT services of all such new arrangements or changes well before such arrangements or changes start to apply. For the same reason, financial entities should have the right to terminate the contract with the ICT third-party service provider where the outcome of their risk assessment shows that the new arrangements or material changes carry a level of risk that exceed their risk tolerance.

(12) The European Supervisory Authorities have conducted an open public consultation on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the ESA's Stakeholder Groups established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([2]), Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([3]), and Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([4]).

(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 ([5]) and delivered an opinion on 20 August 2024,

HAS ADOPTED THIS REGULATION:

Article 1

Overall risk profile and complexity

Financial entities shall take into account their size and their overall risk profile and the nature, scale, and elements of increased or reduced complexity of their services, activities and operations, including elements relating to:

(a) the type of ICT services that support critical or important functions covered by the contractual arrangement between the financial entity and the ICT third-party service provider;

(b) the type of ICT services covered by the contractual arrangement between the ICT-third party service provider and its subcontractors;

(c) the location of the ICT subcontractor providing ICT services that support critical or important functions or a material part thereof, or of its parent company;

(d) the length and complexity of the chain of subcontractors providing ICT services that support critical or important functions or material parts thereof used by the ICT third-party service provider;

(e) the nature of the data shared with the ICT subcontractors providing ICT services that support critical or important functions or material parts thereof;

(f) whether the ICT services that support critical or important functions or material parts thereof are provided by subcontractors, located within a Member State or in a third country, including the location where the ICT services are actually provided from and the location where the data are actually processed and stored;

(g) whether the ICT subcontractors providing ICT services that support critical or important functions or material parts thereof are part of the same group as the financial entity to which those services are provided;

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

(h) whether the ICT subcontractors providing ICT services that support critical or important functions or material parts thereof are authorised, registered or subject to supervision or oversight by a competent authority in a Member State, or are subject to the oversight framework under Chapter V, Section II, of Regulation (EU) 2022/2554;

(i) whether the ICT third-party service providers that support critical or important functions or material parts thereof are authorised, registered or subject to supervision or oversight by a supervisory authority from a third country;

(j) whether the provision of ICT services supporting critical or important functions or material parts thereof is concentrated to a single subcontractor of an ICT third-party service provider or a small number of such subcontractors;

(k) whether the subcontracting of ICT services that support critical or important functions or material parts would impact the transferability of those ICT services to another ICT third-party service provider;

(l) the potential impact of disruptions on the continuity and availability of the ICT services that support critical or important functions or material parts thereof provided by the ICT third-party service provider when using a subcontractor providing ICT services that support critical or important functions or material parts thereof.

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 conditions for subcontracting the use of ICT services that support critical or important functions or material parts thereof, where such subcontracting is permitted under the contractual arrangements on the use of ICT services, are implemented consistently in all financial entities that are part of the group and are adequate for the effective application of this Regulation at all relevant levels.

Article 3

Due diligence and risk assessment regarding the use of subcontractors that support critical or important functions

1. A financial entity shall, before entering into a contractual arrangement with an ICT third-party service provider, decide whether that ICT third-party service provider may subcontract an ICT service that supports critical or important functions or material parts thereof. The financial entity shall only enter into such contractual arrangement where it has assessed that all of the following conditions have been complied with:

(a) the due diligence processes on the ICT third-party service provider ensure that it is able to select and assess the operational and financial abilities of potential ICT subcontractors to provide the ICT services that support critical or important functions or material parts thereof, including by participating, when required to do so by the financial entity, in digital operational resilience testing as referred to in Chapter IV of Regulation (EU) 2022/2554;

(b) the ICT third-party service provider is able to identify all subcontractors that provide ICT services that support critical or important functions or material parts thereof, to notify and inform the financial entity of those subcontractors, and is able to provide to the financial entity all information that may be necessary for the assessment of the conditions under this Article;

(c) the ICT third-party service provider ensures that the contractual arrangements with the subcontractors that provide ICT services that support critical or important functions or material parts thereof enable the financial entity to comply with its own obligations stemming from Regulation (EU) 2022/2554 and applicable Union and national legislation;

(d) the subcontractor grants the financial entity and competent and resolution authorities the same contractual rights of access and inspection as those granted by the ICT third-party service provider;

(e) without prejudice to the financial entity's final responsibility to comply with its legal and regulatory obligations, the ICT third-party service provider itself has sufficient ability, expertise, and adequate financial, human, and technical resources to monitor the ICT risks at the level of subcontractors, including by applying appropriate information security standards and by having in place an appropriate organisational structure, risk management and internal controls, and incidents reporting and responses;

(f) the financial entity has sufficient abilities, expertise, and adequate financial, human and technical resources to monitor the ICT risks relating to the service supporting critical or important functions or material parts thereof that has been subcontracted, including by applying appropriate information security standards and by having in place an appropriate organisational structure and risk management, incident response, business continuity management and internal controls;

(g) the financial entity has assessed the impact on the financial entity's digital operational resilience and financial soundness of a possible failure of a subcontractor that provides ICT services that support critical or important functions or a material part thereof;

(h) the financial entity has assessed the risks associated with the location of the potential subcontractors in relation to the ICT services that support critical or important functions or a material part thereof provided by the ICT third-party service provider;

(i) the financial entity has assessed the ICT concentration risks at entity level in accordance with Article 29 of Regulation (EU) 2022/2554;

(j) the financial entity has assessed whether there are any obstacles to the exercise of audit, inspection and access rights by the competent authorities, resolution authorities, or the financial entity, including persons appointed by them.

2. Financial entities that use ICT third-party service providers that subcontract ICT services that support critical or important functions or material parts thereof shall periodically carry out the risk assessment referred to in paragraph 1, points (f) to (j), against possible changes in their business environment, including against changes in the supported business functions, in risk assessments including ICT threats, ICT concentration risks, and geopolitical risks.

3. Reliance on the results of the risk assessment carried out by their ICT third-party service providers on their subcontractors in complying with the obligations set out in this article shall not limit the final responsibility of financial entities to comply with their legal and regulatory obligations under Regulation (EU) 2022/2554.

Article 4

Conditions under which ICT services that support critical or important functions or a material part thereof may be subcontracted

1. The contractual arrangement concluded between the financial entity and the ICT third-party service provider shall identify which ICT services that support critical or important functions or material parts thereof are eligible for subcontracting and under which conditions. That contract shall specify:

(a) that the ICT third-party service provider is responsible for the provision of the services provided by the subcontractors;

(b) that the ICT third-party service provider is required to monitor all subcontracted ICT services that support critical or important functions or material parts thereof to ensure that its contractual obligations with the financial entity are continuously met;

(c) the monitoring and reporting obligations of the ICT third-party service provider towards the financial entity regarding subcontractors that provide ICT services that support critical or important functions or material parts thereof;

(d) that the ICT third-party service provider is to assess all risks associated with the location of the current or potential subcontractors that provide ICT service that support critical or important functions or material parts thereof, and their parent company and with the location where the ICT service concerned is provided from;

(e) the location of data processed or stored by the subcontractor, where relevant;

(f) that the ICT third-party service provider is to specify in its contract with its subcontractors the monitoring and reporting obligations of that subcontractor towards the ICT third-party service provider, and where agreed, towards the financial entity;

(g) that the ICT third-party service provider is to ensure the continuity of the ICT services that support critical or important functions throughout the chain of subcontractors in case of failure by an ICT subcontractor to meet its contractual obligations;

(h) that the contractual arrangement between the ICT third-party service provider and its subcontractors contains the requirements on business contingency plans referred to in Article 30(3), point (c), of Regulation (EU) 2022/2554 and specifies the service levels to be met by the ICT subcontractors in relation to those plans;

(i) that the contractual arrangement between the ICT third-party service provider and its subcontractors specifies the ICT security standards and any additional security requirements referred to in Article 30(3), point (c), of Regulation (EU) 2022/2554;

(j) that the subcontractor is to grant to the financial entity and relevant competent and resolution authorities the same rights of access, inspection, and audit as those referred to in Article 30(3), point (e), of Regulation (EU) 2022/2554;

(k) that the ICT third-party service provider is to notify the financial entity of any material change to subcontracting arrangements;

(l) that the financial entity has the right to terminate the contract with the ICT third-party service provider when the conditions laid down in either Article 6 of this Regulation or the conditions laid down in Article 28(7) of Regulation (EU) 2022/2554 have been fulfilled.

2. Changes relative to contractual agreements between the financial entity and ICT third-party service providers that provide an ICT service supporting critical or important functions or material parts thereof, made necessary to comply with this Regulation, shall be implemented in a timely manner and as soon as it is possible. The financial entity shall document the planned timeline for the implementation.

Article 5

Material changes to subcontracting arrangements of ICT services that support critical or important functions or material parts thereof

1. The contractual arrangement shall provide that the ICT third-party service provider shall inform the financial entity about any intended material changes to its subcontracting arrangements well in time to enable the financial entity to assess:

(a) the impact on the risks it is or might be exposed to;

(b) whether such material changes might affect the ability of the ICT third-party service provider to meet its contractual obligations vis-a-vis the financial entity.

2. The contractual arrangement shall contain a reasonable notice period by which the financial entity is to approve or object to the changes.

3. The ICT third-party service provider shall only implement the material changes to its subcontracting arrangements after the financial entity has either approved or not objected to the changes by the end of the notice period.

4. Where the financial entity is of the opinion that the material changes referred to in paragraph 1 exceed the financial entity's risk tolerance, the financial entity shall, before the end of the notice period:

(a) inform the ICT third-party service provider thereof;

(b) object to the changes and request modifications to those changes before they are implemented.

Article 6

Termination of the contract between the financial entity and the ICT third-party service provider

The financial entity shall have the right to provide in the contractual arrangement with the ICT third-party service provider that the contractual arrangement is to terminate in each of the following cases:

(a) the financial entity has objected to material changes to the subcontracting arrangements supporting critical or important functions and requested for modifications to those arrangements, but the ICT third-party service provider has nevertheless implemented those material changes;

(b) the ICT third-party service provider has implemented material changes to subcontracting arrangements supporting critical or important functions or material parts thereof before the end of the notice period without approval by the financial entity;

(c) the ICT third-party service provider subcontracts an ICT service that supports a critical or important function or material part thereof not explicitly permitted to be subcontracted by the contract between the financial entity and the ICT third-party service provider.

Article 7

Entry into force

This Regulation shall enter into force on the twentieth day following that of 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, 24 March 2025.

For the Commission
The President
Ursula VON DER LEYEN