This Addendum ("Addendum") contains provisions to ensure that all Parties comply with 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 related delegated and implementing acts ("DORA").

THE PARTIES:

1) BIT B.V., with its registered office at Galileïlaan 19, 6716 BP Ede (the Netherlands), registered with the Dutch Chamber of Commerce under number 09090351 ("BIT"); and

2) , with its registered office at ( ) ("Customer")

BIT and the Customer shall hereinafter be referred to individually as a "Party" and collectively as the "Parties";

WHEREAS:

A) This Addendum applies to those ICT services ("Services") in all Agreements between the Parties to which Regulation (EU) 2022/2554 is applicable;

B) The Customer, as a regulated financial entity under DORA, must ensure its resilience against ICT-related disruptions, threats, and incidents;

C) The Parties acknowledge that the Services support or perform certain critical or important functions (as defined in Article 3(22) of DORA) of the Customer;

D) Pursuant to Article 30(1) of DORA, the Customer and BIT shall clearly specify their respective rights and obligations concerning the Services, including the contractual requirements set out in Article 28(7) and Article 30(2) of DORA;

E) The Parties agree to incorporate this Addendum into the Agreements to ensure compliance with the applicable DORA requirements[1];

F) *If applicable – see Article 11* | The Customer has not been designated by the supervisory authorities as a financial entity subject to Threat-Led Penetration Testing (TLPT) under Article 26 of DORA, and therefore the Parties shall not agree on provisions requiring BIT to participate in or fully cooperate with the Customer's TLPT, as outlined in Article 30(3)(d) of DORA[2];

G) The references to DORA article numbers in this Addendum pertain to the articles of DORA dated 14 December 2022. In the event of amendments to DORA resulting in renumbered articles, the article numbers in this Addendum shall refer to the updated numbering in DORA.

AGREE TO THE FOLLOWING:

Contents

1 DEFINITIONS

1.1 Terms capitalised in this Addendum shall have the meaning ascribed to them in DORA, insofar as such terms are defined therein[3]. All other capitalised terms in this Addendum shall have the following meaning:

- **"Addendum"** means this document, including any annexes.
- **"DORA"** means 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, and related delegated and implementing acts, as amended, supplemented or replaced from time to time.
- **"DORA Effective Date"** means the date on which DORA becomes applicable, being 17 January 2025.
- **"Services"** means the Services as defined in Article 2(21) of DORA, provided by BIT to the Customer under the Agreement.
- **"BIT Website"** means the website of BIT, accessible at www.bit.nl.
- **"Material Change"** means a change in Subcontracting that may significantly impact the availability, confidentiality, integrity, or operational resilience of the Services provided by BIT. This includes the replacement of a Subcontractor, expansion of services by an existing Subcontractor, changes to Service Locations, or other substantial amendments to contractual terms with Subcontractors.
- **"Subcontracting"** means the engagement of a third party by BIT to perform (part of) the Services.
- **"Subcontractor"** means a third party engaged by BIT (or any of its subcontractors) to perform part of the Services.
- **"Agreement"** means the agreement(s) referred to in recital (A) above.
- **"Customer Data"** means all information, including personal data, collected, stored, processed and/or transmitted by or through the use of the Services as provided by BIT.
- **"Portal"** means the BIT customer portal where the Customer can, among other things, manage and view various aspects of the Services and the Service Level Agreement, accessible at portal.bit.nl.

2 APPLICABILITY, INTERPRETATION AND HIERARCHY

2.1 This Addendum shall take effect (i) on the date of execution by both Parties if executed on or after the DORA Effective Date, or (ii) on the DORA Effective Date, if this Addendum is executed prior to such date.

2.2 Upon the effective date of this Addendum, the Agreement shall be amended and/or supplemented by the terms set out in this Addendum. Amendments and/or supplements to Agreements already concluded between the Parties prior to the effective date of this Addendum shall not have retroactive effect. Any rights and obligations already accrued under the Agreement shall therefore remain unaffected.

2.3 This Addendum and the Agreement shall be interpreted in accordance with DORA. In the event of conflicting interpretations between the Parties, BIT's interpretation shall prevail, provided it complies with DORA requirements.

2.4 In the event of any conflict between this Addendum and other provisions of the Agreement, the provisions of this Addendum shall prevail.

3 EXTENSION OF THIS ADDENDUM

3.1 The Parties may extend the applicability of this Addendum to other agreements under which BIT provides Services to the Customer by making an explicit reference to this Addendum, provided that the Parties document in writing any additional amendments necessary to comply with DORA regarding such Services.

3.2 Where the scope of this Addendum is extended, this Addendum shall be incorporated into each of the relevant agreements separately. For clarity: referencing this Addendum in other agreements shall not result in the consolidation of such agreements with the Agreement; each agreement shall remain separate and independent unless the Parties expressly agree otherwise.

4 AMENDEMENT

4.1 The Parties shall amend this Addendum as necessary to maintain compliance with DORA when new or amended laws, regulations or guidelines come into force that conflict with the provisions of this Addendum or the Agreement or otherwise necessitate changes to ensure the Parties' continued compliance with DORA.

4.2 Each Party shall notify the other Party in writing of any changes within the meaning of Article 4.1. The primary responsibility for monitoring such changes lies with the Customer.

4.3 If implementing the required changes or other changes requested by the Customer would affect BIT's operational processes, require (significant) technical changes to the Services, or result in additional costs for BIT, BIT shall have the right to object to such changes by providing a reasoned written notice to the Customer. In the event of an objection, the Parties shall negotiate in good faith to amend the changes and/or agree on additional compensation, subject to compliance with DORA.

5 SCOPE AND LOCATION OF THE SERVICES

5.1 The Services provided by BIT are described in detail in the Agreement and relevant Service Level Agreements[4].

5.2 The (Subcontracted) Services shall be provided in the Netherlands, unless otherwise specifically agreed with the Customer[5].

5.3 BIT shall inform the Customer at least thirty (30) days in advance if BIT intends to change the locations referred to in the preceding paragraph[6]. Such notice shall be published on the BIT Website or through another channel where BIT can prove receipt by the Customer. If BIT provides such notice by email, it shall do so using the email address recorded in BIT's administration as the contact for contractual matters.

6 SUBCONTRACTING

6.1 BIT may subcontract all or part of the Services or make (Material) Changes to the Subcontracting arrangements. BIT shall inform the Customer in advance of engaging a new Subcontractor or planned Material Changes to Subcontracting. Such notice shall be published on the BIT Website or through another channel where BIT can prove receipt by the Customer. If BIT provides such notice by email, it shall do so using the email address recorded in BIT's administration as the contact for contractual matters.

6.2 The Customer has the right to object to the engagement of a new Subcontractor or to Material Changes in Subcontracting. BIT shall provide the Customer with the opportunity to submit a reasoned written objection within thirty (30) days. In the event of an objection, the Parties shall consult in good faith to address the Customer's concerns.

6.3 Either Party may terminate the Agreement and this Addendum with immediate effect by written notice to the other Party if the Customer has objected to Material Changes proposed by BIT to its Subcontracting arrangements and the Parties have failed to reach agreement on the proposed Material Changes within fourteen (14) days after the objection period. If an exit plan is initiated following termination of the Agreement and this Addendum, BIT's implementation of the Material Changes objected to by the Customer shall not constitute a breach of any obligations under the Agreement or this Addendum.

6.4 BIT shall maintain an up-to-date overview of material Subcontractors in the entire chain involved in the provision of the Services and, upon the Customer's written request, provide the legally required information necessary for the Customer to perform the assessments required under DORA, ensuring that by providing such up-to-date information, the Customer can comply with its obligations to maintain and update the information register in accordance with Article 28(3) and 28(9) of DORA.

7 IDENTIFICATION OF THE LEGAL ENTITY[7],[8]

7.1 BIT shall:

a) obtain and maintain a valid and active Legal Entity Identifier (LEI) or European Unique Identifier (EUID) as referred to in Article 16 of Directive (EU) 2017/1132;

b) where relevant, ensure that Subcontractors providing components of the Services provide a valid and active LEI or EUID as referred to in Article 16 of Directive (EU) 2017/1132, unless the Subcontractor is a natural person acting in a business capacity;

c) maintain and/or request the legal identification details of all Subcontractors and provide these to the Customer upon first request.

7.2 Where a legal entity is established outside the European Economic Area, such entity may only be identified with a Legal Entity Identifier (LEI)[9].

8 SERVICE LEVELS

8.1 The service levels for the Services, including precise quantitative and qualitative performance targets and any updates and revisions thereof, are described in the Agreement, specifically in the relevant Service Level Agreements[10],[11].

8.2 The relevant Service Level Agreements describe the performance standards (such as Availability, Response Time and Recovery Time), and the service level-linked obligations shall apply within this framework.

8.3 BIT shall enable the Customer to effectively monitor the Services and verify compliance with the service levels and associated performance targets[12], in accordance with the Service Level Agreement.

8.4 BIT shall promptly notify the Customer in writing of any developments that may materially affect BIT's ability to effectively deliver the Services in accordance with the agreed service levels[13].

9 CUSTOMER DATA

9.1 Customer Data shall be processed and stored in the context of the (Subcontracted) Services in the Netherlands, unless otherwise specifically agreed with the Customer[14].

9.2 BIT shall inform the Customer at least fourteen (14) days in advance if BIT intends to change the locations referred to in the preceding paragraph. Such notice shall be published on the BIT Website or through another channel where BIT can prove receipt by the Customer[15]. If BIT provides such notice by email, it shall do so using the email address recorded in BIT's administration as the contact for contractual matters.

9.3 BIT shall take measures to ensure the availability, authenticity, integrity and confidentiality of all Customer Data processed in the context of the (Subcontracted) Services, in accordance with the measures and provisions set out in the Agreement.

9.4 In the event of insolvency, winding-up or cessation of business operations of BIT, or termination of the Agreement for any reason, the Customer shall have the right to access and control the Customer Data processed or stored in the context of the (Subcontracted) Services as set out in the Agreement.

9.5 Upon the Customer's request following any of the events referred to in Article 9.4, BIT shall provide the Customer Data in an easily accessible format within (i) ninety (90) calendar days after termination of the Agreement by BIT or (ii) within thirty (30) calendar days after termination of the Agreement by the Customer, either by enabling the Customer to export the Customer Data itself or by providing the Customer with a data export[16].

9.6 Upon termination of the Agreement, BIT may irreversibly delete Customer Data. If the Customer objects to such deletion, BIT may agree to retain the Customer Data for an additional retention period of up to ninety (90) calendar days, unless a longer period is agreed in writing, subject to the Customer's payment of reasonable additional (storage) costs, to be agreed between the Parties prior to the additional retention period, or, in the absence of such specific agreement, based on BIT's standard rates for such or similar activities.

10 TRAINING AND AWARENESS

10.1 BIT agrees to participate in ICT security awareness programmes and training on digital operational resilience (hereinafter: "Training") if the Customer has included external ICT service providers as participants in its training programme[17],[18]. BIT shall participate for reasonable compensation. The aforementioned compensation shall be based on BIT's standard rates for such or similar activities.

10.2 If BIT is expected to participate in one or more Training sessions, BIT shall be notified in writing by the Customer at least sixty (60) calendar days in advance. In consultation, the Parties shall determine a suitable date for the Training(s). Generally, participation may not be required more than once per calendar year, unless the given situation reasonably warrants more frequent Training. Participation shall in any event not be required if BIT can reasonably demonstrate that the relevant Training is unnecessary because the relevant knowledge is already present within BIT's organisation, or if the Customer is inflexible in determining the date and BIT cannot participate due to time constraints or other valid reasons. BIT shall communicate this in writing, whereupon the Parties shall consult to reach agreement.

10.3 The obligation to participate in Training is limited to persons directly involved in or responsible for the provision of the (subcontracted) Services and persons with direct or indirect access to Customer Data, including its direct management. However, a maximum of three (3) BIT employees may participate per Training to avoid adversely affecting business continuity. If the Customer requires more than three (3) BIT employees to participate, the Parties shall consult to reach agreement, including the possibility of spreading the Training(s) over multiple days.

10.4 The Customer shall ensure that the Training can be attended remotely via video conference, unless the nature of the Training reasonably requires physical attendance. Training dates, times and locations shall be arranged in a manner that reasonably accommodates BIT's business interests and operational needs.

11 IT SECURITY, BUSINESS CONTINUITY PLANS AND TESTING

11.1 BIT shall implement, maintain and periodically test a business continuity plan appropriate to the nature of the Services provided, covering at least the continuity and availability of the Services and Customer Data[19].

11.2 BIT shall implement security measures, tools and policies that, in BIT's professional judgement, provide an appropriate level of security within the meaning of Article 30(3)(c) of DORA, taking into account the nature of the Services and commercially reasonable practices in the sector, such as ISO 27001. BIT may modify the implemented ICT security measures from time to time, provided such modifications do not reduce the security of the Services.

11.3 [IF APPLICABLE] BIT shall participate in and provide full cooperation with the Customer's threat-led penetration testing ("TLPT") as referred to in Articles 26 and 27 of DORA, insofar as the Services provided by BIT are within the scope of a TLPT[20]. The Parties acknowledge that TLPT may reasonably adversely affect the quality or security of services provided to BIT's customers not subject to DORA, or the confidentiality of data relating to such services. The Parties therefore agree as follows:

11.3.1 The Customer shall notify BIT in writing, where reasonably possible at least sixty (60) calendar days prior to a TLPT in which BIT is required to participate;

11.3.2 The Customer shall not request BIT to participate in a TLPT more than once per year;

11.3.3 The Customer shall bear all costs and expenses associated with the TLPT, including but not limited to BIT's reasonable personnel costs at BIT's then-current rates and other reasonable costs incurred by BIT; and

11.3.4 The Customer shall indemnify and hold BIT harmless from all claims, damages and costs (including reasonable legal costs) arising from or related to a TLPT.

12 IT RELATED INCIDENTS

12.1 BIT shall promptly notify the Customer after becoming aware of an ICT-related incident. The Customer shall designate at least one contact person for BIT to notify of such ICT-related incidents. The names and contact details of these persons are recorded in BIT's administration.

12.2 In the event of an ICT-related incident affecting or relating to the Services, BIT shall, upon the Customer's first request and without undue delay, provide all assistance required under DORA[21].

12.3 In the event of an ICT-related incident caused by the Customer and affecting or relating to the Services, BIT shall, upon the Customer's first request and without undue delay, provide all assistance required under DORA for reasonable compensation. The aforementioned compensation shall be based on BIT's standard rates for such or similar activities.

13 AUDITS AND COOPERATION

13.1 BIT hereby agrees to grant the Customer, its authorised representatives and relevant supervisory authorities access to documentation critical to the provision of BIT's Services for inspection, audit and copying. Such access to documentation shall not include documentation relating to intellectual property and confidential (business) information; BIT shall not provide access to such documentation. BIT shall ensure that such rights are not restricted or impeded by other contractual arrangements or policies[22].

13.2 The Customer and BIT acknowledge that circumstances may arise where access, inspection or audit rights adversely affect the rights of BIT's other customers. The Parties agree that in such cases, they may agree in writing on alternative inspection options. The Parties shall cooperate in good faith in such circumstances to establish appropriate alternative options, protecting the legitimate interests of BIT's other customers[23].

13.3 BIT shall:

13.3.1 Provide full cooperation to the competent authorities and resolution authorities (including persons designated by them) supervising the Customer under DORA[24],[25];

13.3.2 Provide full cooperation and reasonable assistance during on-site inspections and audits conducted by the competent authorities, the lead overseer, the Customer or their appointed representatives, provided such representatives are subject to appropriate confidentiality obligations;

13.3.3 Upon request, grant effective access to the Customer, its internal and external auditors and the relevant competent authorities to data and premises relating to the use of the Services provided under the Agreement[26].

13.4 The Customer shall not conduct an audit or inspection at BIT more than once per calendar year.

13.5 The Customer shall notify BIT in writing at least sixty (60) calendar days in advance of any Customer-initiated inspection or audit, unless such prior notice is not reasonably possible due to exceptional circumstances requiring immediate action. In such a situation, the Customer shall inform BIT as soon as possible with the knowledge and information available at that time.

13.6 Prior to a Customer-initiated inspection or audit, BIT and the Customer shall endeavour to agree in writing on the scope and areas to be audited, applicable procedures, confidentiality requirements and operational guidelines to be followed during (on-premises) inspection or audit activities[27]. In any event, such written agreement shall address the aspects set out by BIT in the standard security testing agreement, as described at https://www.bit.nl/en/about-bit/terms-and-policies/security-test-agreement/.

13.7 The Customer shall bear all costs and expenses associated with Customer-initiated inspections or audits, including but not limited to BIT's reasonable personnel costs at BIT's then-current professional services rates and other reasonable costs incurred by BIT.

13.8 All information, knowledge and documentation obtained and shared through audits or inspections shall be treated confidentially by the Parties.

14 EXIT[28]

14.1 Notwithstanding any other exit strategies, exit plans or similar arrangements included in the Agreement – which shall prevail if more favourable to the Customer – BIT shall, upon the Customer's written request, continue to provide the Services after the expiry or termination of the Agreement for an appropriate transition period taking into account all circumstances and the legitimate interests of both Parties.

14.2 The duration of the transition period shall be determined by the Customer and notified to BIT in writing and shall not exceed six (6) months, unless a longer period is required to reduce the risk of disruption to the Customer's business operations or to ensure the effective resolution and restructuring of the Customer. The originally determined transition period may be extended by mutual agreement.

14.3 During the transition period, BIT shall continue to provide the Services under the same service levels, prices and terms as specified in the Agreement. At the Customer's request, BIT shall provide reasonable assistance in migrating the Services to a successor service provider or the Customer's internal solution, to the extent reasonably possible. The Customer shall reimburse BIT for all reasonable costs and expenses incurred in providing such migration assistance at BIT's then-current professional services rates.

15 TERMINATION

15.1 Notwithstanding any other termination rights available to the Parties under the Agreement or applicable law, either Party may terminate the Agreement and this Addendum:

a) By written notice with immediate effect, in the circumstances described in Article 28(7) of DORA[29];

b) By written notice, provided that (i) the terminating Party has been requested by the competent (resolution) authority to terminate the Agreement, and (ii) a notice period equal to the maximum notice period prescribed by such competent (resolution) authority is observed, or in the absence of such prescribed notice period, the relevant notice period as set out in the Agreement[30].

15.2 Termination rights under the Agreement shall be interpreted and exercised in accordance with the applicable expectations of the competent authorities within the meaning of Article 30(2)(h) of DORA[31].

15.3 If the Agreement is terminated under or interpreted in accordance with this Article 15, the Customer shall, without any right of set-off, immediately (i) pay to BIT all outstanding fees for Services provided prior to the termination effective date, and (ii) pay to BIT all unpaid fees covering the remainder of the Agreement's term as if it had not been terminated, with all such amounts becoming immediately due and payable upon termination, to the extent permissible under applicable law.

16 GOVERNING LAW AND JURISDICTION

16.1 This Addendum shall be governed by Dutch law. The courts in the region where BIT has its statutory seat shall have exclusive jurisdiction.

SIGNATURES

BIT B.V.	CUSTOMER
Signature:	Signature:
Name:	Name:
Date:	Date:

17 REFERENCES

[1]Art. 30(1) DORA: "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.".

[2]Art. 30(3)(d) DORA: "the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;"

[3]Art. 30(2)(d) DORA: "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".

[4]Art. 30(2)(a) DORA: "a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider (...)".

[5]Art. 30(2)(b) DORA: "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 (...)".

[6]Art. 30(2)(b) DORA: "(...) and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations".

[7]Art. 3(5) ITS on the register of information (OJ L, 2024/2956): "Financial entities shall use a valid and active legal entity identifier (LEI) or the European Unique Identifier referred to in Article 16 of Directive (EU) 2017/1132 ('EUID'), and where available both of these identifiers, to identify all of their ICT third-party service providers that are legal persons, except for individuals acting in a business capacity.".

[8]Art. 3(6) ITS on the register of information (OJ L, 2024/2956): "Where an ICT service provided by a direct ICT third-party service provider is supporting a critical or important function of the financial entities, financial entities shall ensure through the direct ICT third-party service provider, that all the subcontractors of the direct ICT third-party service provider included in the register of information in accordance with paragraph 2, point (b), which effectively underpin/support ICT services supporting critical or important functions, use a valid and active LEI or provide their EUID, and where available both of these identifiers, except if those subcontractors are individuals acting in a business capacity.".

[9]Recital (9) ITS on the register of information (OJ L, 2024/2956): "(...) whereas the ICT third-party service providers established in third-countries should be identified with LEI only.".

[10]Art. 30(2)(e) DORA: "service level descriptions, including updates and revisions thereof".

[11]Art. 30(3)(a) DORA: "full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels (...)".

[12]Art. 30(3)(a) DORA: "(...) 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".

[13]Art. 30(3)(b) DORA: "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 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".

[14]Art. 30(2)(b) DORA: "the locations, namely the regions or countries (...) where data is to be processed, including the storage location (...)".

[15]Art. 30(2)(b) DORA: "(...) and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations".

[16]Art. 30(2)(d) DORA: "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".

[17]Art. 30(2)(i) DORA: "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)".

[18]Art. 13(6) DORA: " Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i)"

[19]Art. 30(3)(c) DORA: "requirements for the ICT third-party service provider to implement and test business contingency plans (...)".

[20]Art. 30(3)(d) DORA: "the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27".

[21]Art. 30(2)(f) DORA: "the obligation of the ICT third-party service provider to provide assistance to the financial 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".

[22]Art. 30(3)(e)(i) DORA: "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".

[23]Art. 30(3)(e)(ii) DORA: "the right to agree on alternative assurance levels if other clients' rights are affect".

[24]Art. 30(2)(g) DORA: "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".

[25]Art. 3(8)(c) RTS on ICT third-party contractual arrangements (OJ L 2024/1773): "(...) are to require that the ICT third party service providers cooperate with the competent authorities".

[26]Art. 3(8)(d) RTS on ICT third-party contractual arrangements (OJ L 2024/1773): "(...) 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".

[27]Art. 30(3)(e)(iv) DORA: "the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits.".

[28]Art. 30(3)(f) DORA: "exit strategies, in particular the establishment of a mandatory adequate transition period: (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; (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".

[29]Art. 28(7) DORA: "Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances: (a) significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms; (b)

circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider; (c) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data; (d) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement".

[30]Art. 30(2)(h) DORA: "(...) 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".

[31]Art. 30(2)(h) DORA: "(...) 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".