

Memorandum of Understanding on cooperation, exchange of information and coordination of oversight activities of critical ICT third-party service providers located in the European Union and the United Kingdom

between

The European Supervisory Authorities, namely:

the European Banking Authority,
the European Insurance and Occupational Pensions Authority, and
the European Securities and Markets Authority

on the one part,

and

The UK Financial Authorities, namely:

the Bank of England,
the Prudential Regulation Authority, and
the Financial Conduct Authority on the other part,

Collectively the “**Authorities**” and individually an “**Authority**”.

Preamble

- (1) The European Supervisory Authorities (“**ESAs**”) include the European Banking Authority (“**EBA**”) established by Regulation (EU) No 1093/2010¹, the European Insurance and Occupational Pensions Authority (“**EIOPA**”), established by Regulation (EU) No 1094/2010² and the European Securities and Markets Authority (“**ESMA**”) established by Regulation (EU) No 1095/2010³, these three regulations being hereinafter collectively referred to as the “**ESAs Regulations**”.
- (2) The United Kingdom financial Authorities (the “**UK Financial Authorities**”) include the Bank of England (“**BoE**”), the Prudential Regulation Authority (“**PRA**”) and the Financial Conduct Authority (“**FCA**”). Unless otherwise stated, references in this Memorandum of Understanding (“**MoU**”) to the BoE do not include the BoE acting in its capacity as the PRA. References in this MoU to the PRA are to the BoE in its capacity as the PRA.
- (3) Regulation (EU) 2022/2554⁴ (the “**Digital Operational Resilience Act**” or “**DORA**”) establishes a comprehensive framework to ensure the digital operational resilience of financial entities within the European Union (“**EU**”). This Regulation sets out requirements for financial entities with regards to the management of information and communication technology (“**ICT**”) risks, incident reporting, and third-party risk management, to safeguard the financial sector against cyber threats and ICT disruptions.
- (4) DORA attributes an oversight role to the ESAs over ICT third-party service providers designated as critical to the European financial sector (“**critical ICT third-party service providers**” or “**CTPPs**”). The oversight role is attributed to one of the ESAs for each CTPP under the name of Lead Overseer.
- (5) The UK has a corresponding, although distinct, regime under Part XVIII, Chapter 3C of the Financial Services and Markets Act 2000 (“**FSMA**”), that establishes a framework for the oversight by the UK Financial Authorities of critical third parties (“**CTPs**”) designated by HM Treasury (the “**UK CTP Regime**”). In accordance with section 312L FSMA, HM Treasury may designate any person who provides services to UK financial entities as a CTP if in HM Treasury’s opinion a failure in, or disruption to, the provision of those services could threaten the stability of, or confidence in, the UK financial system.
- (6) FSMA attributes an oversight role to the UK Financial Authorities with respect to CTPs once designated by HM Treasury. The UK Financial Authorities have issued substantively identical rules for CTPs, a joint Supervisory Statement and expectations and other guidance outlining

¹ 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 of 15.12.2010, p.12).

² 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 of 15.12.2010, p.48).

³ 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 of 15.12.2010, p.84).

⁴ 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 (OJ L 333 of 27.12.2022, p.1).

their requirements and expectations for CTPs. These are set out in a November 2024 joint policy statement (PRA PS16/24 and FCA PS24/16⁵). Pursuant to FSMA, the UK Financial Authorities share this role and are required to co-ordinate their functions. A Memorandum of Understanding between the UK Financial Authorities dated October 2024⁶ (as amended from time to time) sets out in general terms the exercise of their functions in relation to CTPs and how they intend to coordinate their functions. Under that Memorandum of Understanding the UK Financial Authorities envisage that they may jointly agree that one of them may perform the role of lead regulator for a designated CTP. The UK Financial Authorities are also each responsible for the monitoring of third-party risk in the financial sector in respect of UK financial entities under their supervision.

- (7) This MoU lays down the principles as well as the purpose and scope of international cooperation and exchange of information between the ESAs and the UK Financial Authorities, in relation to the oversight of CTPs and CTPs and in the context of monitoring of third-party risk in the financial sector.
- (8) Under the DORA oversight framework, the ESAs may exercise oversight powers towards CTPs by way of different examinations, such as requests for information, general investigations and on-site inspections.
- (9) In accordance with Article 31(12) of DORA, EU financial entities are only permitted to use the services of a CTP located outside of the EU (a “**non-EU CTP**”) if such a CTP has established an EU subsidiary within 12 months of its designation. The EU subsidiary will serve as the primary contact point and addressee of the ESAs’ oversight measures in relation to the non-EU CTP. The powers conferred to the Lead Overseer under Article 35(1) of DORA include information requests addressed to the EU subsidiary and may concern any information related to the provision of services to EU financial entities by the non-EU CTP, irrespective of whether the information sought to be obtained is stored within the EU or not.
- (10) In the case of a non-EU CTP, the ESAs will focus their oversight activities by addressing the EU subsidiary of this CTP, or any other of its EU subsidiaries. In the case where the ESAs cannot attain their oversight objectives through the EU subsidiaries and wish to conduct an on-site inspection at any CTP premises located in the UK, the ESAs will coordinate their activities with the UK by following the specifications laid down in this MoU.
- (11) The UK Financial Authorities’ approach to the oversight of CTPs will comprise a range of oversight activities including reviews of CTPs’ self-assessments (interim and annual) and supporting documentation; regular and ad-hoc meetings with the CTP; deep dive and thematic reviews (including skilled persons reports); use of powers, including information gathering and referrals to enforcement; participation in incident management playbook exercises (including any feedback provided to the CTP after the exercise); and consideration of incident reports and follow-up actions. Some of these oversight activities may occasionally require on-site access by the UK Financial Authorities, or persons appointed on their behalf (such as skilled persons), to the EU subsidiary, or any other European subsidiaries of a CTP that is also designated as a CTP

⁵ <https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-policy-statement>

⁶ [Memorandum_of_Understanding_between_the_FCA_and_the_Bank_of_England-critical-third-party.pdf](#)

by the ESAs. Where this is the case, the UK Financial Authorities will coordinate their activities with the ESAs by following the specifications laid down in this MoU.

- (12) Article 36(2) of DORA requires the ESAs to conclude administrative cooperation arrangements with the relevant non-EU authorities to enable a smooth conduct of on-site inspections. Article 36(2) of DORA establishes the minimum scope of such cooperation arrangements. Such arrangements may not create legal obligations in respect of the EU and its Member States, nor prevent Member States and their competent authorities from concluding bilateral or multilateral arrangements with those non-EU countries and their relevant authorities.
- (13) Article 44(1) of DORA enables the ESAs to conclude administrative arrangements with non-EU regulatory and supervisory authorities to foster international cooperation on ICT third-party risk mitigation across different financial sectors, in particular by developing best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses. Correspondingly, the UK Financial Authorities view cooperation with non-UK authorities as a key part of the UK CTP Regime. This cooperation contributes to the effective oversight of CTPs and promotes interoperability with other regimes aimed at managing systemic risks to the financial system posed by third party service providers. This cooperation can also reduce duplicative oversight of CTPs/CTPPs, and promote a more efficient use of resources by the Authorities, other relevant authorities and CTPs/CTPPs.
- (14) Under Article 49 of DORA, the ESAs have established a pan-European systemic cyber incident coordination framework (“**EU-SCICF**”), with the objective of facilitating an EU-coordinated response in case of major cyber incidents with a potential systemic impact. This operational/strategic framework foresees the establishment of communication channels with international stakeholders that will need to be defined and effectively structured within cooperation agreements to allow for exchange of information.
- (15) Likewise, under the UK CTP Regime, effective incident management is vital for ensuring that CTPs manage potential systemic risks when responding to major incidents (referred to as CTP operational incidents in the UK Financial Authorities’ rules). CTPs will be required to cooperate with the UK Financial Authorities and affected UK financial entities to coordinate responses to CTP operational incidents, including through Collective Incident Response Frameworks. Strengthening communication and coordination between the UK Financial Authorities, the ESAs and the various relevant incident coordination and response frameworks in the EU and UK during CTP operational incidents and major ICT-related incidents with systemic and cross-border impact is another key objective of this MoU.
- (16) Effective cooperation relies on the possibility to share information freely and safely among authorities, and this is facilitated by robust provisions on professional secrecy. The confidentiality and professional secrecy regime applicable to the UK has been assessed by the ESAs to be equivalent to the respective EU framework.
- (17) Nothing in this MoU restricts or prevents the Authorities from sharing information to assist each other in carrying out their functions as may be permitted by law, either under other Memoranda of Understanding between the Authorities or otherwise.

- (18) The Authorities intend to ensure an effective level of cooperation and exchange of information, and, where appropriate, coordination of the ESAs' oversight activities carried out under DORA and the UK Financial Authorities' oversight of CTPs under the UK CTP Regime, and for this purpose have decided to enter into this MoU.

Article 1

Purpose and scope of cooperation

1. This MoU lays down the principles and key areas for cooperation and exchange of information between the ESAs and the UK Financial Authorities, in relation to the oversight of CTPPs under DORA and CTPs under the UK CTP Regime, including but not limited to the coordination of the ESAs' and UK Financial Authorities' oversight activities addressed at CTPPs owning, or using in any way, premises located in the UK for providing services to EU financial entities, and CTPs owning, or using in any way, premises located in the EU for providing services to UK financial entities. Such cooperation will assist the Authorities to manage risks to the stability of, or confidence in, their respective financial sectors.
2. This MoU also aims to foster cooperation and exchange of information including in emergency situations, between the ESAs and the UK Financial Authorities on ICT third-party risk across different financial sectors, in particular, with the aim of developing best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses.

Article 2

Definitions

For the purposes of this MoU:

- a) **'Authority/ies'** means a signatory/ies to this MoU or any successor thereto.
- b) **"Books and Records"** means documents, electronic media, and books and records within the possession, custody and control of a CTPP or CTP.
- c) **"Collective Incident Response Framework"** means any group involving UK financial entities, the UK Financial Authorities or a combination thereof, whose purpose is to facilitate a collective response to incidents that may adversely affect the UK's financial sector.
- d) **"Critical ICT third-party service provider"** or **"CTPP"** means an ICT third-party service provider designated as critical in accordance with Article 31 of DORA.
- e) **"Critical third party"** or **"CTP"** means a critical third party designated by HM Treasury under section 312L(1) of FSMA.
- f) **"EU financial entities"** means the entities referred to in Article 2(1), points (a) to (t), of DORA, which are located in the EU.
- g) **"ICT third-party service provider"** means an undertaking providing information and communication technology ("**ICT**") services.
- h) **"Jurisdiction"** means for the ESAs the EU and for the UK Financial Authorities the UK.

- i) **“Mutually Designated CTP/CTPP”** means a CTPP which has also been designated as a CTP.
- j) **“On-site inspections”** means the oversight activities, powers and proceedings referred to in Article 39 of DORA where the ESAs enter into CTPP premises in the UK or oversight tasks under FSMA, including information-gathering and investigation, where a UK Authority enters into CTP premises in the EU.
- k) **“Onward sharing authority”** means any authority listed in paragraph 1 of Appendix B to this MoU.
- l) **“Oversight tasks”** means work, activities or actions conducted by, in the case of the EU, the Lead Overseer and its designated staff in order to achieve the objectives set out in Article 33 of DORA, including the exercise of powers referred to in Article 35 of DORA; and in the case of the UK, the UK Financial Authorities under their functions in relation to CTPs in accordance with Part XVIII, Chapter 3C of FSMA.
- m) **“Secure Electronic Means”** means electronic methods of communications that ensure that completeness, integrity and confidentiality of information are maintained during transmission.
- n) **“Traffic Light Protocol” or “TLP”** means the categorisation of information according to four labels each related to sensitiveness and indicating the sharing limitations to be applied by the recipients: TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR⁷.
- o) **“UK financial entities”** means authorised persons, relevant service providers or FMI entities as referred to in section 312L(1) FSMA.

Article 3

General principles for cooperation and exchange of information

1. For Mutually Designated CTPs/CTPPs, each Authority will use best endeavours to provide the Authorities of the other jurisdiction, on a timely basis upon request or on its own initiative, where appropriate and insofar as legally possible and operationally feasible, with any information that is, in the Authority’s reasonable view, material to the exercise of the other Authorities’ oversight tasks. For CTPs/CTPPs which are not mutually designated, each Authority may provide, where appropriate and insofar as legally possible and operationally feasible, material information to the Authorities of the other jurisdiction—either upon request or proactively—to support the other Authorities’ oversight tasks.
2. Where necessary, the Authorities will reasonably assist the other jurisdiction’s Authorities in interpreting such information so as to enable them to assess compliance with the laws or regulations to which the CTPs/CTPPs are subject.
3. Each Authority will endeavour to provide the Authorities of the other jurisdiction, insofar as practicable and as permitted by law, regulation or other requirements, with assistance in engaging with non-cooperative Mutually Designated CTPs/CTPPs headquartered in the EU or UK. Any relevant assistance will be without prejudice to the ability of each Authority to exercise its respective legal powers or employ other methods, if necessary, to address

⁷ In the case of disclosures by the UK Financial Authorities, “TLP: CLEAR” may be labelled as “TLP: BLUE”.

non-cooperation by a CTP/CTPP subject to its oversight, in line with Article 11 (Legal Nature).

Article 4

Mechanisms for the transmission of any relevant information

1. The exchange of information between the Authorities referenced in Article 3 (General principles for cooperation and exchange of information) is primarily intended to be conducted in writing by Secure Electronic Means.
2. The Authorities intend to use the ESAs' oversight collaboration tool, where mutually agreed, for such exchanges of information. The ESAs' oversight collaboration tool is a dedicated Secure Electronic Means provided by the ESAs for the communication and exchange of information for each of the Authorities' oversight tasks under this MoU and which presents technical information security measures to guarantee the confidentiality of data against unauthorised access. Where the ESAs' oversight collaboration tool is not available or agreed, other Secure Electronic Means including encrypted email will be used. In urgent situations, requests may be made orally, provided that they are subsequently confirmed in writing by Secure Electronic Means, and provided such oral communication is restricted to necessary recipients.
3. To enhance the quality of co-operation and assistance, the Authorities may convene ad hoc meetings to discuss material issues of common concern in relation to CTPs/CTPPs and coordinate actions, if deemed appropriate.
4. Both the request for exchange of information and the communication of the requested information will be addressed to the designated contact persons as set forth in Appendix A unless otherwise agreed to by the Authorities.
5. In requesting an exchange of information, the Authorities should clarify at least the following:
 - a) the information sought by the requesting Authority;
 - b) a concise description of the facts underlying the request;
 - c) the purpose for which the information is sought;
 - d) the reasons why the information is relevant for the proper performance of the requesting Authority's tasks;
 - e) the time limit within which the information is to be provided and, where appropriate, the urgency thereof; and
 - f) to whom, if anyone, including any governmental entity, onward disclosure of information is likely to be necessary and the reasons for any such disclosure.
6. Information and documentation shared should adhere to the TLP categorisation. In cases where no label is specified, the information will be treated as confidential. The Authorities

that are parties to this MoU agree to primarily handle information according to the TLP categorisation. The Authorities, where appropriate, seek to categorise information based on the categorised TLP sensitivity level assigned by the originating Authority. The adoption of TLP as a framework for information sharing should not preclude the application of the security procedures delineated in each of the internal classification policies of the Authorities to this MoU.

7. Where a request for exchange of information cannot be fulfilled or the information requested is not available, the Authority that has received that request will endeavour to provide the reasons for not sharing the information.

Article 5

Procedures for the coordination of on-site inspections by the ESAs

1. The ESAs may seek to conduct on-site inspections of CTPPs on any premises located in the UK, which are owned or used by such CTPPs in any way for the purposes of providing services to EU financial entities, when the ESAs' oversight objectives cannot be attained by means of interacting with the relevant subsidiary located within the EU or other EU subsidiaries, or by exercising oversight activities on premises located in the EU.
2. The conduct of on-site inspections by the ESAs referred to in paragraph 1 is subject to all of the following conditions in accordance with Article 36(1), second subparagraph of DORA:
 - a) the conduct of the inspection in the UK is deemed necessary by the ESAs to allow it to fully and effectively perform its oversight duties in line with DORA;
 - b) the inspection in the UK is directly related to the provision of ICT services to EU financial entities;
 - c) the relevant CTPP consents to the conduct of the inspection in the UK; and
 - d) the relevant UK Authority has been officially notified by the ESAs and raised no objection thereto.
3. For any Mutually Designated CTPs/CTPPs, the UK Financial Authorities will endeavour to assist the ESAs, where consent of the relevant CTPP to the on-site inspection has been obtained by the ESAs, as far as practicable with the conduct of on-site inspections of CTPPs including notifying the ESAs of their non-objection, if appropriate.
4. For any CTPPs which have not also been designated as CTPs in the UK, the UK Financial Authorities will not be a relevant authority for the purposes of the ESA's notification under Article 36(1)(b)(iv) of DORA. Any response, or lack of response, by a UK Financial Authority to a communication regarding a CTPP which has not been designated as a CTP in the UK will not be considered as objection or non-objection for this purpose. The UK Financial Authorities will endeavour to provide the ESAs with the contact details of the appropriate UK authority within a reasonable time, or advise if no such authority exists.

5. For the purposes of the preceding paragraph, the UK Financial Authorities will provide the ESAs with a list of relevant UK non-financial authorities which to the best of their knowledge could constitute the relevant contacts.
6. Once the relevant alternative UK authority is identified, the ESAs will be responsible for coordinating bilaterally with these relevant alternative UK authorities.
7. The ESAs will duly notify the UK Financial Authorities of any plans to conduct on-site inspections as soon as practicable and in any event no later than three weeks before the initiation of the inspection or investigation, and at least six weeks in advance for a non-urgent inspection or investigation. This notification will detail to the best of the ESAs' knowledge:
 - a) the name and other relevant information of the CTPP subject to the inspection;
 - b) the legal basis, including the relevant decision ordering the inspection;
 - c) the scope, subject matter and purpose of the inspection;
 - d) the expected starting and ending dates of the inspection; and
 - e) the names and contact details of the designated individuals who will take part in the inspection.
8. When the ESAs notify the UK Financial Authorities of an on-site inspection of a Mutually Designated CTP/CTPP and the consent of the relevant CTPP to the on-site inspection has been obtained, the UK Financial Authorities will endeavour to cooperate with the ESAs in relation to the execution of the inspection. The ESAs will act in accordance with the following procedure before conducting such an on-site inspection:
 - a) To the extent not already provided under paragraph 7, the ESAs will inform the UK Financial Authorities on the intended timeframe for, the scope, subject matter and purpose of the on-site inspection.
 - b) When establishing the subject matter of an on-site inspection, the ESAs will consider the monitoring or supervisory activities of the UK Financial Authorities and will consider any information or documentation that was made available or is capable of being made available by the UK Financial Authorities.
 - c) The UK Financial Authorities will endeavour to respond promptly to the ESAs notification of intention to conduct an on-site inspection. Where practicable, the UK Financial Authorities will, within 15 business days, acknowledge receipt of the ESAs notification and indicate the timeframe for providing the response if it cannot be given within that period. Where the UK Financial Authorities do not communicate a response to the notification within 15 business days, the ESAs may deem this as a non-objection to the on-site inspection. For the purpose of the UK Financial Authorities' non-objection, the UK Financial Authorities will inform the ESAs which UK Financial Authority will be responsible for notifying the non-objection to the ESAs' on-site inspection on a case by case basis.
 - d) When requested by the ESAs and agreed with the UK Financial Authorities, the UK Financial Authorities may assist with the review of the contents of public or non-

public Books and Records, including documents and electronic data, and information obtained from management and staff of the CTPP, where applicable.

9. On conclusion of the on-site inspection, the relevant ESA performing such activities may present the UK Financial Authorities with their findings within a reasonable timeframe. The above-mentioned information will be given insofar as possible and subject to applicable laws and regulations, and in line with the principles set out in this MoU.

Article 6

Procedures for the coordination of on-site inspections by the UK Financial Authorities

1. The UK Financial Authorities may seek to conduct on-site inspections, or other oversight activities requiring on-site access, of CTPs on any premises located in the EU, which are owned or used by such CTPs in any way for the purposes of providing services to UK financial entities, when their oversight objectives cannot be attained by exercising oversight activities on premises located in the UK.
2. For any Mutually Designated CTPs/CTPPs, the ESAs will endeavour to assist the UK Financial Authorities, as far as practicable, with the conduct of on-site inspections in the EU. Such assistance will also include assistance to any third party commissioned by the UK Financial Authorities, where such person is covered by the UK's professional secrecy regime, including persons appointed by the UK Financial Authorities under Part XI (Information Gathering and Investigations) of FSMA, such as skilled persons under section 166 of FSMA.
3. For any CTPs which have not also been designated as CTPPs in the EU, the ESAs will endeavour to provide the requesting UK Financial Authority with the contact details of the relevant financial or non-financial authority in the EU, or advise if no such authority exists.
4. For the purposes of the preceding paragraph, the ESAs will provide the UK Financial Authorities with a list of relevant financial or non-financial authorities in the EU which to the best of their knowledge could constitute the relevant contacts.
5. Once a relevant EU financial or non-financial authority is identified, the UK Financial Authorities will be responsible for coordinating bilaterally with the relevant EU financial or non-financial authority.
6. The UK Financial Authorities will duly notify the ESAs of any plans to conduct on-site inspections as soon as practicable and in any event no later than three weeks before the initiation of the inspection or investigation, and at least six weeks in advance for a non-urgent inspection or investigation. This notification will detail to the best of the UK Financial Authorities' knowledge:
 - a) the name and other relevant information of the CTP subject to the inspection;
 - b) the legal basis, including the relevant decision ordering the inspection;
 - c) the scope, subject matter and purpose of the inspection;
 - d) whether the CTP has consented to the inspection;

- e) the expected starting and ending dates of the inspection; and
 - f) the names and contact details of the designated individuals who will take part in the inspection.
7. When the UK Financial Authorities notify the ESAs of an on-site inspection of a Mutually Designated CTP/CTPP, the ESAs will endeavour to cooperate with the UK Financial Authorities in relation to the execution of the inspection. The UK Financial Authorities will act in accordance with the following procedure before conducting such an on-site inspection:
- a) To the extent not already provided under paragraph 6, the UK Financial Authorities will inform the ESAs on the intended timeframe for, the scope, subject matter and purpose of the on-site inspection.
 - b) When establishing the subject matter of an on-site inspection, the UK Financial Authorities will consider the oversight activities of the ESAs and will consider any information or documentation that was made available or is capable of being made available by the ESAs.
 - c) The ESAs will endeavour to respond promptly to the UK Financial Authorities' notification of intention to conduct an on-site inspection. Where practicable, the ESAs will, within 15 business days, acknowledge receipt of the UK Financial Authorities' notification.
 - d) When requested by the UK Financial Authorities and agreed with the ESAs, the ESAs may assist with the review of the contents of public or non-public Books and Records, including documents and electronic data, and information obtained from management and staff of the CTP, where applicable.
8. On conclusion of the on-site inspection, the relevant UK Financial Authority performing such activities may present the ESAs with their findings within a reasonable timeframe. The above-mentioned information will be given insofar as possible and subject to applicable laws and regulations, and in line with the principles set out in this MoU.

Article 7

Mechanism for notification in cases of infringement or non-compliance by Mutually Designated CTPs/CTPPs

- 1. If a UK Financial Authority deems that a Mutually Designated CTP/CTPP has infringed the requirements to which it is obliged to adhere pursuant to applicable UK law when providing services to financial institutions in the UK, it will notify the ESAs in accordance with paragraph 3.
- 2. If an ESA deems that a Mutually Designated CTP/CTPP has not complied with ESAs oversight measures in accordance with Article 35(1) of DORA, or deems that a Mutually Designated CTP/CTPP has infringed the requirements to which it is obliged to adhere pursuant to applicable EU law when providing services to financial institutions in the EU, it will notify the UK Financial Authorities in accordance with paragraph 4.
- 3. For the purposes of paragraph 1:

- a) a UK Financial Authority should notify the ESAs promptly once it has decided to appoint investigators under section 168(5) FSMA to conduct an investigation into a potential contravention by a Mutually Designated CTP/CTPP of a requirement imposed upon it under Chapter 3C (Critical Third Parties) of Part XVIII of FSMA; and
 - b) upon the conclusion of that investigation, the notifying UK Financial Authority should promptly notify the ESAs its decision whether to impose sanctions under section 312Q (Power of Censure) or section 312R (Disciplinary Measures) FSMA on the Mutually Designated CTP/CTPP.
- 4. For the purposes of paragraph 2, an ESA should notify the UK Financial Authorities promptly where:
 - a) a Mutually Designated CTP/CTPP is not following a recommendation addressed to it by the Lead Overseer or has not declared its intention to follow such recommendation, and where the Lead Overseer, pursuant to Article 42(1) of DORA, has informed the relevant EU competent authorities accordingly;
 - b) the Lead Overseer has adopted a decision imposing a periodic penalty payment in accordance with Article 35(6) of DORA; or
 - c) the Lead Overseer has issued a public disclosure in accordance with Article 42(2) of DORA.
- 5. The notification should include at least the following elements if they are available at the time of notification, and the notifying Authority should provide any remaining elements as soon as possible:
 - a) the nature of the alleged infringement or non-compliance;
 - b) the timing of the investigation or other action by the Authority concerned, including any applicable period of hearing the CTP/CTPP; and
 - c) any other information it considers relevant in connection with the alleged infringement or non-compliance.
- 6. Following a recommendation of the Lead Overseer, as referred to in paragraph 4, and subject to the consent from relevant EU competent authorities, the ESAs will share information, as soon as practicable, in relation to an EU competent authorities' decisions addressed at financial entities, to temporarily suspend, either in part or completely, the use or deployment of a service provided by a Mutually Designated CTP/CTPP or to terminate, in part or completely, the relevant contractual arrangements concluded with a Mutually Designated CTP/CTPP in accordance with Article 42(6) of DORA.
- 7. The UK Financial Authorities will accordingly use best endeavours to notify the ESAs in advance of any decision on their part that would have an equivalent effect to a partial or complete suspension of use or deployment of a service or partial or complete termination of contractual arrangements referred to in paragraph 6.
- 8. The Authorities will also inform each other, as appropriate, if they are aware of any failure by a Mutually Designated CTP/CTPP to cooperate effectively with the Authorities.

9. Where, after providing a notification, the notifying Authority becomes aware of the submission of a remedial plan, the notifying Authority will share relevant details of such plan with the Authorities of the other jurisdiction or inform such other Authorities as soon as practicable.
10. Where, after providing a notification pursuant to the above provisions, the notifying Authority becomes aware that the alleged infringement or non-compliance does not materialise, or makes a finding to this effect, or elects to discontinue its investigation into the alleged infringement or non-compliance, the notifying Authority will share relevant details of this with the Authorities of the other jurisdiction as soon as practicable.

Article 8

Oversight methodologies and topics of common interest

1. The Authorities endeavour to cooperate in establishing mechanisms to share effective practices or relevant methodologies relevant to the oversight of CTPPs and CTPs.
2. The Authorities further endeavour to exchange views on emerging technologies and topics of common interest, as deemed relevant by them.

Article 9

Updates on regulatory or supervisory developments on the monitoring of ICT third-party risk of financial sector entities in the UK and EU

1. The Authorities, where appropriate, intend to share information regarding ICT third-party risk across the different financial sectors in their respective jurisdictions that is likely to be of assistance to them for their oversight of CTPs/CTPPs, in order to promote the safe and sound operation of major ICT third-party service providers and develop best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses.
2. In particular, the Authorities may exchange information in circumstances where issues of regulatory, supervisory or enforcement concern may arise and are relevant to their respective oversight of CTPs/CTPPs, including but not limited to:
 - a) relevant oversight activities, such as planned on-site inspections, included in the annual oversight plan for a CTPP or for the CTP in the year ahead;
 - b) relevant material oversight activities not scheduled in advance;
 - c) supervisory assessments of compliance and monitoring of the ongoing compliance by CTPPs or CTPs with legal and regulatory requirements;
 - d) regulatory, supervisory or enforcement actions or approvals taken by the Authorities or notified to the Authorities with prior consent, in relation to the oversight of CTPPs or CTPs;

- e) planned changes to the relevant obligations and requirements to which CTPPs or CTPs are subject.
3. Exchanges of information under paragraphs 1 and 2 will take place in accordance with Article 4 (Mechanisms for the transmission of any relevant information).
 4. This MoU is without prejudice to the Authorities' pre-existing ability to transmit updates on regulatory or supervisory developments on the monitoring of ICT third-party risk of financial institutions. The Authorities envisage that discussions on ICT third-party risk will also continue under separate cooperation agreements and between teams which are not directly involved in CTP/CTPP oversight.

Article 10

Cooperation in relation to emergency situations

1. The Authorities will use best endeavours to:
 - a) inform each other promptly if they become aware of an emerging or existing emergency situation in relation to a CTP or CTPP including, but not limited to:
 - i. significant disruption at a CTP or CTPP, which might have an adverse impact on EU financial entities or UK financial entities, including but not limited to a CTP operational incident under the UK Financial Authorities' rules or a major ICT-related incident with systemic impact; and
 - ii. serious legal, regulatory, operational or financial difficulties of a CTP or CTPP which might have an adverse impact on EU financial entities or UK financial entities;
 - b) exchange information relating to the emergency situation, including but not limited to reports of CTP operational incidents under the UK Financial Authorities' rules or summaries or extracts thereof, and any relevant incident information obtained from CTPPs;
 - c) where appropriate, seek coordinated responses to any existing or emerging crisis involving a CTP or CTPP in their respective jurisdictions, in accordance with the applicable legislation and without prejudice to their respective involvement in the relevant cross-border cooperation fora;
 - d) where appropriate, collaborate with financial sector incident response frameworks in their respective jurisdictions; and
 - e) identify and share lessons learnt from relevant emergency situations.
2. Where appropriate, the Authorities may agree to take part in joint oversight activities aimed at improving the ability of CTPs, CTPPs or the wider financial sector to respond to and recover from major disruption, including but not limited to observing incident management playbook exercises of CTPs.

Article 11

Legal nature

1. This MoU is a statement of intent to consult, cooperate, exchange information and coordinate activities in connection with the Authorities' supervisory/oversight competences as regards the ongoing compliance by CTPPs and CTPs with the applicable requirements to which they are subject in their jurisdictions, as well as with the Authorities' monitoring of related regulatory or supervisory developments.
2. The cooperation and information sharing arrangements under this MoU should be interpreted and implemented in a manner that is permitted by and consistent with, the laws and other legal or regulatory requirements applicable to each Authority.
3. This MoU does not create any legally binding obligations, confer any rights or supersede any domestic or EU laws. This MoU does not confer upon any person the right or ability, directly or indirectly, to obtain, suppress or exclude any information or to challenge the execution of a request for assistance under this MoU.
4. This MoU is not intended to limit or condition the discretion of an Authority in any way in the discharge of its regulatory or supervisory responsibilities or to prejudice or affect in any way the individual responsibilities, competencies or autonomy of any Authority. This MoU does not limit an Authority to taking solely those measures described herein in fulfilment of its responsibilities and mandates. In particular, this MoU does not affect any right of any Authority to communicate with or obtain information or documents from any person subject to its oversight or supervision that is located in the territory of the other Authority.
5. The Authorities should, within the framework of this MoU, provide each other with the fullest cooperation permissible under their laws and regulations in relation to their respective oversight competencies in relation to CTPPs or CTPs, as well as to the monitoring of related regulatory and supervisory developments in each of their respective jurisdictions.
6. Following consultation, cooperation may be denied:
 - a) where the cooperation would require an Authority to act in a manner that would violate laws and regulations applicable to it; or
 - b) where the cooperation would be unduly burdensome; or
 - c) on the grounds of UK public interest for UK Financial Authorities or of European public interest for the ESAs.
7. The Authorities represent that, as of the date of this MoU, no domestic or EU laws or regulations should prevent them from providing assistance of the nature provided for in this MoU to one another.

8. The Authorities will endeavour to reach an understanding on the interpretation and application of this MoU. Where the Authorities encounter material differences of views related to the interpretation of a provision of this MoU, they should endeavour to make good faith efforts, through cooperation, consultations and discussions, to resolve such differences in order to reach a mutually acceptable resolution of the issues raised.
9. To facilitate communication and cooperation under this MoU, the Authorities hereby designate contact persons as set forth in the Appendix A. Any modifications to the details of contact persons should be communicated without undue delay to the other Authorities.

Article 12

Confidentiality and permissible uses of information

1. The Authorities acknowledge that all information exchanged on the basis of this MoU may be confidential information within the meaning of the legal framework applicable to the Authorities. The Authorities acknowledge that all information exchanged on the basis of this MoU shall be treated as if it is confidential unless otherwise agreed in writing.
2. The Authorities will preserve the confidentiality of the information received as far as legally possible, except as provided in this MoU or pursuant to a legally enforceable demand. Any confidential information received by the Authorities under this MoU will be used exclusively by the relevant Authorities for the exercise of their functions, including their functions in relation to CTPPs or CTPs and will not be disclosed to third parties except as set out below.
3. Each Authority will ensure that all persons that deal with or have access to confidential information provided by the other Authority (including any of its staff, members of its governance bodies, external providers and any persons who perform tasks on behalf of such Authority that have access to confidential information) are bound by the obligations of confidentiality and professional secrecy in compliance with the applicable legal framework, including after the termination of their duties.
4. Except as provided in paragraphs 5 and 6, before any Authority that has received confidential information under this MoU (a “**receiving Authority**”) discloses any confidential information, categorised as TLP:AMBER or TLP:RED, received from another Authority to a third party, the receiving Authority will request and obtain prior written consent, which will not be unreasonably withheld, from the Authority that provided the information. Before disclosing the confidential information to such a third party (including in a situation provided for in paragraph 5), the receiving Authority will obtain a commitment from that party that information will be kept confidential. During an emergency situation, consent may be obtained in any form, including orally, provided such communication is confirmed in writing as promptly as possible.
5. If the receiving Authority is legally required to disclose confidential information received under this MoU to a third party, it will, to the extent permitted by law, inform the Authority that provided the information about such possible onward sharing, including the purposes for which the information is going to be shared, the uses that the third party

could make of the information and the safeguards that the third party would put in place to ensure the confidentiality of the information. If the Authority that provided the information under this MoU does not consent to the disclosure to a third party, then the receiving Authority will take reasonable steps to resist disclosure, including by employing legal means to challenge the request for disclosure or by advising the third party of the possible negative consequences that such disclosure might have on the future exchange of confidential information between the Authorities.

6. Subject to the conditions set out in Appendix B, where either an ESA or a UK Financial Authority transmits information received to an onward sharing authority, it will notify the Authority which provided the information, ideally before the transmission of the information and, at the latest, within 15 days from such transmission.
7. The Authorities intend that the sharing or disclosure of confidential information, including deliberative and consultative materials, pursuant to the terms of this MoU, will not constitute a waiver of privilege or confidentiality of such information.

Article 13

Processing of Confidential Information

1. The Authorities represent and acknowledge that under the terms of this MoU:
 - a) the ESAs process confidential information in accordance with the relevant provisions of EU law, including the ESAs Regulations, and internal requirements on confidentiality and professional secrecy;
 - b) The UK Financial Authorities process confidential information in accordance with the relevant provisions of UK law, including FSMA, and internal requirements on confidentiality and professional secrecy.

Article 14

Data Protection

1. The Authorities would process personal data for which they are controllers in accordance with the applicable data protection laws and regulations. The ESAs would process the personal data in line with Regulation 2018/1725 (EUDPR).
2. The transfers of personal data between ESAs and the UK Financial Authorities would be based, for the ESAs, on Chapter V of Regulation 2018/1725 (EUDPR).
3. The UK Financial Authorities would process personal data in accordance with data protection and privacy legislation (including subordinate legislation) in force from time to time in the UK, including but not limited to the assimilated law version of the General Data Protection Regulation (EU) 2016/679 (UK GDPR) and the Data Protection Act 2018. Accordingly, for the UK Financial Authorities, transfers of personal data between the UK and ESAs would be conducted in accordance with Chapter V of the UK GDPR.

Article 15

Successor authorities

1. Where the relevant functions of an Authority are transferred or assigned to another authority or authorities, the terms of this MoU shall apply to the successor authority or authorities performing those relevant functions, such successor authority or authorities shall become a signatory or signatories to this MoU without the need for any further amendment to this MoU, and notice will be provided to the other Authorities.
2. This will not affect the right of any Authority to give written notice as provided in Article 17 (Termination) that it no longer wishes to be a signatory to this MoU if it wishes to do so.

Article 16

Amendments

1. The Authorities intend to periodically review the functioning and effectiveness of this MoU between the Authorities, including in consideration of changes in the regulatory status or supervisory treatment of CTPPs or CTPs in the relevant regulatory or supervisory regime in either jurisdiction.
2. This MoU may be amended with the written consent of all Authorities. By derogation from the need to obtain written consent from all Authorities, amendments to the relevant contact point listed in Appendix A can be made by each Authority giving written notice to the other Authorities.

Article 17

Termination

1. This MoU will remain operative, unless terminated, for an unlimited period of time.
2. If an Authority wishes to no longer be a signatory to this MoU, it shall provide 30 calendar days prior written notice to the other Authorities.
3. If an Authority gives such notice, the parties will consult concerning the disposition of any pending requests for information or assistance. If an agreement cannot be reached through consultation, cooperation will continue with respect to all requests for information or assistance that were made under this MoU before the expiration of the 30-day period until all requests are fulfilled or the requesting Authority withdraws such request(s).
4. In the event of termination of this MoU, any confidential information obtained under this MoU will continue to be treated in the manner described under Article 12 (Confidentiality and permissible uses of information).

Article 18

Publication

1. This MoU may be made publicly available in full or in part by any of the Authorities at any time and in any manner.

Article 19

Entry into operation

1. This MoU will come into effect at the latest of the dates on which this MoU is signed by the Authorities.

Executed by the Authorities.

For the European Banking Authority

Jose Manuel Campa, Chairperson

For the European Insurance and Occupational
Pensions Authority

Petra Hielkema, Chairperson

For the European Securities and Markets
Authority

Verena Ross, Chair

For the Bank of England

Sarah Breeden, Deputy Governor for Financial
Stability

For the Financial Conduct Authority

Nikhil Rathi, Chief Executive

For the Prudential Regulation Authority

Sam Woods, Chief Executive

Appendix A
Contact Persons (redacted)

Appendix B

Onward sharing Authorities

1. *List of Onward Sharing Authorities*

For the purposes of Article 12(6) of this MoU, “**onward sharing authorities**” means any of the authorities listed below, when fulfilling the conditions which are set out in paragraph 2 of this Appendix:

EU Authorities

- a) competent authorities referred to in Article 46 of DORA;
- b) the EBA, ESMA, EIOPA, and the European Systemic Risk Board (“**ESRB**”);
- c) resolution authorities referred to in Article 2(1), point 18 of Directive 2014/59/EU⁸; and
- d) competent authorities, single points of contact and the computer security incident response teams (“**CSIRTs**”) designated or established in accordance with Directive (EU) 2022/2555⁹.

UK Authorities

- a) the UK Financial Authorities;
- b) His Majesty’s Treasury (HMT);
- c) National Cyber Security Centre (NCSC) including in its capacity as Single Point of Contact (SPOC) and/or Computer Security Incident Response Team (CSIRT);
- d) Competent authorities under the Network and Information Systems Regulations 2018 and any future or successor legislation. In particular, the Information Commissioner’s Office (ICO) and Office of Communications (OFCOM);
- e) any other departments of His Majesty’s Government (HMG), public bodies and agencies to the extent necessary for coordinating an incident response, such as those responsible for protecting critical infrastructure or responding to major crimes; and
- f) successor authorities to any of the authorities referred to in a) to d).

2. *Condition*

For the purposes of Article 12(6) of this MoU, an authority listed in paragraph 1 of this Appendix shall be considered as an onward sharing authority under the condition that the confidential information is transmitted only where necessary for the performance of the disclosing authorities’ lawful monitoring or supervisory tasks over for the UK Financial Authorities, CTPs, or for the ESAs, CTPPs. This paragraph does not apply in respect of onward sharing between the Authorities.

The information received shall in any event be subject, in accordance with applicable law, to professional secrecy requirements at least equivalent to those applicable to the UK Financial

⁸ Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms (OJ L 173, 12.6.2014, p. 190–348).

Authorities (in respect of information which a UK Financial Authority has shared onward) or the ESAs (in respect of information which an ESA has shared onward).

In addition to such professional secrecy requirements as may be required by law, confidential information will not be further disclosed by the onward sharing authority, except to other authorities listed in paragraph 1 of this Appendix, and subject to the obligation to notify the Authority which provided the information in accordance with Article 12(6) of this MoU or as authorised by an Authority in accordance with Article 12(5) of this MoU.

3. *Notification*

By way of derogation to Article 12(6) of this MoU, no notification is required for the ESAs or the UK Financial Authorities where information is shared:

- a) within their organisation and governance; or
- b) for the ESAs, within the European System of Financial Supervisors as referred to in Article 2(2) of the ESAs Regulations,
- c) for the UK Financial Authorities, among the UK Financial Authorities for the purposes of carrying out the functions set out in paragraph 2 of this Appendix.