Joint controllership arrangements with regard to the processing of personal data in connection with the operation of the central database established pursuant to Article 9a of Regulation (EU) No 1093/2010

Having regard to Regulation (EU) No 1093/2010 of the Eureropean 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 ('the EBA Regulation') [1], in particular Article 9a;

Having regard to Commission Delegated Regulation (EU) 2024/595 of 9 November 2023 supplementing Regulation (EU) No 1093/2010 of the European Parliament and of the Council with regard to regulatory technical standards specifying the materiality of weaknesses, the type of information collected, the practical implementation of the information collection and the analysis and dissemination of the information contained in the Anti-money laundering and counter terrorist financing (AML/CFT) central database referred to in Article 9a(2) of that Regulation ('the Article 9a RTS');

Having regard to 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 ('EUDPR');

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR');

I. BACKGROUND

1. Whereas, pursuant to Article 9a of the EBA Regulation and the Article 9a RTS,

   - the EBA is mandated to lead, coordinate and monitor the EU financial sector's fight against money laundering and terrorist financing and, as part of this mandate, the EBA is mandated, amongst other matters, to establish and keep up to date a central anti-money laundering and countering the financing of terrorism database in the terms of point (a) of paragraph 1 of Article 9a of the EBA Regulation ('EuReCA').

   - The Reporting Authorities, as such term is defined in Article 1(1) of the Article 9a RTS, are obliged to provide information to the EBA to feed EuReCA and may request from the EBA, information processed on this database.

[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, 15.12.2010, p. 12.

2. Whereas, for these purposes, pursuant to recital 21 of the Article 9a RTS, the EBA, of one part, together with each Reporting Authority, ESMA and EIOPA of the other part (together, 'the Parties') enter into these Arrangements with regard to the processing of personal data in connection with the operation of EuReCA. These Arrangements do not affect the responsibilities of the Parties under Union or Member State law.

II. SCOPE, DEFINITIONS AND INTERPRETATION

3. These Arrangements apply to processing operations relating to personal data transferred between the Parties to or from EuReCA. The Arrangements are designed to determine in a transparent manner the respective responsibilities of the Parties as joint controllers for compliance with their data protection obligations in relation to EuReCA for the purposes of Article 28 of EUDPR and Article 26 of GDPR.
4. The definitions set out in Article 3 of EUDPR and Article 4 of GDPR respectively apply for the purpose of these Arrangements.

5. For the avoidance of doubt, and in line with Article 9a of the EBA Regulation and the Article 9a RTS, unless otherwise determined in these Arrangements, these Arrangements shall be interpreted so that:

- The EBA shall be responsible for the compliance with data protection obligations when it processes personal data to analyse the information provided by Reporting Authorities pursuant to the Article 9a RTS, and to operate, store and maintain this database and its supporting infrastructure, and;

- The other parties shall be responsible for the compliance with data protection obligations when they process personal data to provide information to the EBA to feed this database, and when they process personal data in the context of a request of information where such personal data has been provided to them by the EBA or when the EBA has shared information on its own initiative with them.

III. LEGAL BASIS AND PURPOSES

6. The Parties acknowledge that the lawfulness of the processing of personal data will be in accordance with Article 5(1)(a) and (b) of the EUDPR and Article 6(1)(c) and (e) of the GDPR, having regard to Article 9a of the EBA Regulation and to the Article 9a RTS which provide for the transfer and use of information, including personal data, by the Parties.

7. The Parties acknowledge that processing operations should be carried out only to the extent necessary to support the purposes set out in the Article 9a RTS ('agreed purposes').

IV. PERMITTED RECIPIENTS

8. The Parties may give access to personal data only to authorised members of their staff or, where necessary, other persons carrying out tasks for the Parties on a contractual basis, for the legitimate performance of tasks which are compatible with the purposes set out above.

V. RECORDS, INFORMATION, COOPERATION, SECURITY, RETENTION AND STORAGE

9. The Parties undertake to maintain complete and accurate records and information to demonstrate compliance with these Arrangements.

10. In the areas described below, the Parties undertake:
    a) Information and cooperation:
        i) to provide reasonable assistance to each other in complying with their respective obligations under the EUDPR and GDPR and applicable data protection rules;
        ii) to ensure that personal data that they report in EuReCA is accurate and remains accurate when processed;
        iii) to limit their processing to what is necessary for the agreed purposes;
        iv) to provide information to any data subject whose personal data may be processed by them in relation to the operation of this database to the extent that this is considered appropriate pursuant to the EUDPR and GDPR respectively. In any case, EBA shall make publicly available a privacy statement in respect of the processing of personal data pursuant to Article 9a RTS;
        v) to ensure that the essence of these Arrangements is made available to data subjects;
        vi) to provide each other with up-to-date contact details for a single point of contact for queries, complaints and provision of information between the Parties within the scope of these Arrangements;[2]
        vii) to publish up-to-date contact details for a single point of contact whom data subjects can contact when they wish to exercise their rights under the EUDPR and GDPR respectively.

    b) Security:
        i) to implement appropriate technical and organisational measures, designed to:
            - ensure and protect the security, integrity and confidentiality of the personal data in their respective possession;

[2] The contact point for the purpose of these Arrangements shall be the same contact point as provided under the Article 9a RTS. Contact point for authority indirectly submitting information to the EBA is the contact point provided to the authority enabling indirect submission.

- protect against any unauthorised or unlawful processing, loss, use, disclosure or acquisition of or access to any personal data in their respective possession.

ii) to ensure that all permitted recipients are subject to statutory or written contractual obligations concerning the shared personal data (including obligations of confidentiality).

11. Article 14 of the Article 9a RTS sets out obligations regarding storage limitation and deletion of personal data. Personal data will be stored and processed by the EBA exclusively within the EEA. The EBA shall request other Parties on an annual basis that they review personal data that they have reported, in particular special categories of data such as suspicions of offences and criminal convictions, in order to ensure that it remains relevant, accurate and up-to-date and to consider whether they should request its deletion.

VI. REQUESTS FROM DATA SUBJECTS

12. The Parties shall provide each other with reasonable assistance in complying with any data subject requests relating to personal data processed through EuReCA.

13. Where a Party other than the EBA receives such a data subject request, it shall forward the request (or the part of the request that concerns the personal data processed through EuReCA) promptly to the following EBA mailbox eureca@eba.europa.eu.

14. The EBA shall process such data subject requests with the assistance, where necessary, of the Reporting Authority which reported to the EBA the personal data to which the data subject request refers, and with any other authority that has received some or all of that personal data from EuReCA. The EBA will decide with those authorities on whether, and to which extent, there are grounds to grant or restrict a particular data subject request. In the event the Party which received the data subject request is other than the EBA or the Reporting Authority that reported the personal data, the EBA shall seek to inform such Party of the decision adopted on the request (or of the need for more time to handle the request) and the reasoning behind it, without undue delay, and, at the latest, 7 calendar days before the time periods, specified in Article 14(3) of the EUDPR and Article 12(3) of the GDPR, expire.

15. The Party which received the data subject request shall be responsible for replying to that request on the basis of the information communicated by the EBA without undue delay and at the latest within the time periods specified in Article 14(3) of the EUDPR or, where applicable, Article 12(3) of the GDPR. Should more time be required to handle the request for justified reasons in particular to ensure that any appropriate restrictions on the right to of access in accordance with Article 25 of the EUDPR and Article 23 of the GDPR are taken into account, the data subject shall receive a holding reply. To ensure consistency, upon request from the Party which received the data subject request, the EBA, where possible, shall prepare a draft reply.

16. The Parties shall not disclose or release personal data in response to a data subject access request without first consulting each other where it is considered relevant and reasonably possible to do so.

VII. DATA BREACHES

17. The Parties shall provide each other with reasonable assistance as required to facilitate the handling of any data breach in application of Article 34 and 35 of the EUDPR, or Article 33 and 34 of the GDPR, as appropriate.

18. Each Party is responsible for personal data breaches that occur as a result of an infringement of that Party's obligations under these Arrangements and, as applicable, the EUPDR and the GDPR.

19. Any Party which becomes aware of a personal data breach affecting this database shall notify the EBA without undue delay and, at the latest, within 24 hours after becoming aware, notwithstanding any ongoing investigations on the applicable causes or on the mitigation measures to be adopted to mitigate the risks to the rights and freedoms of data subjects.

20. Where appropriate, the EBA shall notify the personal data breach to the other Parties, informing them of any measures taken in that context to mitigate the risk to the rights and freedom of data subjects.

21. The Parties shall provide each other with reasonable assurance that they have an effective procedure to identify and manage data breaches internally.

22. The EBA, notwithstanding the cause of the personal data breach shall notify, as applicable, the European Data Protection Supervisor within 72 hours from becoming aware of the breach. In the event other Reporting Authorities, including the Party responsible for the personal data breach, consider necessary to notify their respective data protection authorities as well, they will inform the EBA in advance to make sure the approach is consistent. The Party responsible for the personal data breach, in cooperation with the EBA, shall notify data subjects of the data breach where required to do so under the EUDPR or the GDPR.

VIII. RESTRICTIONS ON RIGHTS OF DATA SUBJECTS

23. To the extent necessary to preserve the useful effect of restrictions imposed with respect to personal data by one Party pursuant to Article 25 of the EUDPR or Article 23 of the GDPR, the other Party shall apply those restrictions provided that it may lawfully do so.

24. Data subjects shall be informed of such restrictions in accordance with, as applicable, Article 25 of the EUDPR or the legislative measure referred to in Article 23(1) of the GDPR.

IX. SETTLEMENT OF DISPUTES, AND LIABILITY

25. These Arrangements are governed by Union law. In accordance with Article 82 of the GDPR where more than one controller is involved in the same processing and is responsible for any damage caused by processing, each shall be held liable for the entire damage, and may claim back from the other controller involved that part of the compensation corresponding to their part of responsibility for the damage.

26. The Parties shall endeavour to settle amicably any dispute arising out of or relating to the interpretation or application of these Arrangements. If at any time a question, dispute or difference arises between the Parties, in relation to or in connection with these Arrangements, the Parties will use every endeavour to resolve it by a process of consultation. The preference is that all disputes are settled at the operational level as they arise.

27. The purpose of the consultation shall be to review and agree so far as is practicable the action taken to solve the problem arisen and the Parties shall negotiate with each other in good faith to that end.

28. If the dispute cannot be settled amicably, each Party may submit for mediation and/or judicial proceedings in the following manner:
    (a) in case of mediation, the Parties shall jointly appoint a mediator acceptable by each of them, who will be responsible for facilitating the resolution of the dispute within two months from the referral of the dispute to him/her;
    (b) in case of judicial proceedings, the matter shall be referred to the Court of Justice of the European Union in accordance with Article 272 of the Treaty on the Functioning of the European Union.

29. The parties which are Union institutions, agencies and bodies are liable for non-compliance in line with Chapter VIII of the EUDPR. The other parties are liable for non-compliance in line with Chapter VIII of the GDPR.

X. ENTRY INTO APPLICATION OF AND AMENDMENTS TO THE ARRANGEMENT

The Arrangement shall apply from the date notified to the other Parties by the EBA. The EBA shall provide a copy of the Arrangement to the Parties at least one month before that date and shall ask them to acknowledge the Arrangement and confirm that they will implement it.

The Arrangement may be amended or supplemented by the EBA. The EBA shall provide a draft proposal for agreement to AMLSC at least three months before the changes are

proposed to take place and shall provide at least one month's notice to the Parties of the final changes unless such changes are required in order to comply with legislative requirements. The EBA shall ask the other Parties to acknowledge the updated requirements and that they will implement the changes.