



COMMISSION IMPLEMENTING REGULATION (EU) 2024/607

of 15 February 2024

on the practical and operational arrangements for the functioning of the information sharing system pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council ('Digital Services Act')

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) ⁽¹⁾, and in particular Article 85 thereof,

After consulting the Digital Services Committee in accordance with Article 88 of Regulation (EU) 2022/2065,

Whereas:

- (1) Regulation (EU) 2022/2065 seeks to ensure a safe digital space for users, while ensuring that fundamental rights are respected. It does this by imposing obligations on providers of intermediary services to prevent the spread of illegal content online and by regulating those providers' content moderation policies in relation to their services. The effective supervision, investigation, enforcement and monitoring of those providers' compliance with those obligations requires cooperation between the Member States and with the Commission, as well as a seamless exchange of information between the Member States and with the Commission.
- (2) To this end, Article 85 of Regulation (EU) 2022/2065 requires the Commission to establish and maintain a reliable, secure and interoperable information sharing system, hereinafter 'AGORA', that supports communications between Digital Services Coordinators, the Commission and the European Board for Digital Services ('the Board'). Other competent authorities may be granted access to AGORA, where necessary, to carry out the tasks conferred on them in accordance with Regulation (EU) 2022/2065. The Digital Services Coordinators, the Commission, and the Board are required to use AGORA for all communications made pursuant to Regulation (EU) 2022/2065.
- (3) AGORA is a software application accessible via the Internet to be developed by the Commission. AGORA provides a communication mechanism to facilitate the cross-border exchange of information and mutual assistance between Digital Services Coordinators, the Commission and the Board pursuant to Regulation (EU) 2022/2065. In particular, AGORA should support the Digital Services Coordinators, the Commission and the Board in managing the exchange of information in connection with the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065 based on simple and unified procedures.
- (4) This Regulation sets out the practical and operational arrangements for the set-up, maintenance and operation of AGORA for the purposes of supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065, which may cover, inter alia, one-to-one exchange of information, notification procedures, alert mechanisms, mutual assistance arrangements and problem-solving between Digital Services Coordinators, the Commission, the Board, and other competent authorities that have been granted access to AGORA pursuant to Regulation (EU) 2022/2065 ('AGORA actors').
- (5) Given the cross-border and cross-sectoral relevance of intermediary services, a high level of coordination and cooperation among the different relevant actors is necessary to ensure the consistent supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065, and the availability of relevant information through AGORA for that purpose.

⁽¹⁾ OJ L 277, 27.10.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2065/oj>.

- (6) In order to overcome language barriers, AGORA should be available in all official languages of the Union. To that end, AGORA should offer fully automated machine-translation tools currently available to the Commission for the translation of documents and messages exchanged through it. The Commission should provide natural persons working under the authority of Digital Services Coordinators, the Commission, the Board or other competent authorities that have been granted access to AGORA ('AGORA user'), and AGORA users appointed as administrators by the Digital Services Coordinators, the Commission, and the Board ('AGORA administrator') with such tools. The automated machine-translation tools should be compatible with the security and confidentiality requirements for the exchange of information in AGORA.
- (7) In order to fulfil their tasks under Regulation (EU) 2022/2065, Digital Services Coordinators, the Commission and the Board may need to exchange information which may include personal data. Any such exchange of information should comply with the rules on the protection of personal data laid down in Regulations of the European Parliament and of the Council (EU) 2016/679 ⁽²⁾ and (EU) 2018/1725 ⁽³⁾. Accordingly, the exchange of personal data necessary to comply with the obligations and to fulfil the tasks laid down in Regulation (EU) 2022/2065 falls within the scope of the lawful processing of data pursuant to Article 5, point (a) of Regulation (EU) 2018/1725, and Article 6(1), point (e) of Regulation (EU) 2016/679.
- (8) AGORA should be the tool used for the exchange of information, including, where necessary, personal data, which would otherwise take place via other means, including regular mail or electronic mail on the basis of a legal obligation imposed on Digital Services Coordinators, the Commission, the Board, and other competent authorities that have been granted access to AGORA pursuant to Regulation (EU) 2022/2065. Personal data exchanged via AGORA should only be processed for the purpose of the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065. Where personal data is processed in the operation of AGORA for the purposes of sharing, requesting and accessing information answering requests for information, referrals, requesting action and requesting support, the Digital Services Coordinators should be separate controllers within the meaning of Regulation (EU) 2016/679 for the processing activities they carry out.
- (9) Each Digital Services Coordinator may also decide to use AGORA for its own case-handling activities carried out for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065. Where personal data is not to be exchanged in AGORA for the purposes of sharing, requesting and accessing information, answering requests for information, referrals, requesting action and requesting support, each Digital Services Coordinator and, where applicable, other competent authorities that have been granted access to AGORA, should be a sole controller within the meaning of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 with respect to the data processing activities carried out by means of AGORA.
- (10) The transmission, storage, and other processing of personal data of natural persons should take place in AGORA for the purposes of supporting communications between AGORA actors to carry out case-handling activities by them in connection with the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.
- (11) AGORA should process personal data insofar as strictly necessary for the supervision, investigation, enforcement, and monitoring under Regulation (EU) 2022/2065. AGORA should process personal data, such as identification data (e.g., name, nickname, alias, date of birth, place of birth, nationality, identification documents, and where necessary other characteristics likely to assist in identification), contact details (e.g., professional and private address, e-mail address, and telephone), case involvement data (e.g., the position and function of the natural person in an undertaking, other roles such as suspect, victim, whistleblower, informant, and witness), case related data (e.g., document, image, video, voice recording, statement, opinion, and record) and any other information deemed necessary to fulfil the requirements under Regulation (EU) 2022/2065.

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

⁽³⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

- (12) Following the data protection-by-design and by-default principles, AGORA should be developed and designed with due respect to the requirements of data protection legislation, in particular due to restrictions imposed on access to personal data exchanged in AGORA. Therefore, AGORA should offer a considerably higher level of protection and security than other methods of information exchange, such as telephone, regular mail, or electronic mail.
- (13) The Commission should supply and manage the software and IT infrastructure for AGORA, ensure its reliability, security, availability, maintenance and operation, and be involved in the training of and technical assistance to AGORA administrators and AGORA users.
- (14) The competence of the Member States to decide which national authorities carry out the obligations resulting from this Regulation should be exercised in accordance with Article 49 and Article 62 of Regulation (EU) 2022/2065. Member States should be able to adapt functions and responsibilities in relation to AGORA to reflect their internal administrative structures, and to implement in AGORA a specific type of work or order of stages in a given work process.
- (15) Each Digital Services Coordinator should appoint and notify the Commission at least one AGORA administrator in its Member State for issues relating to AGORA. Each Digital Services Coordinator should also be responsible for the appointment of AGORA administrators of its respective competent authorities that have been granted access to AGORA pursuant to Regulation (EU) 2022/2065. Each AGORA administrator should register, grant and revoke access to AGORA to its own AGORA users. In order to achieve efficient supervision, investigation, enforcement and monitoring cooperation of services in scope of Regulation (EU) 2022/2065 through AGORA, Member States should ensure that their respective AGORA administrators and AGORA users have the necessary resources to carry out their obligations in accordance with Article 50(1) of Regulation (EU) 2022/2065.
- (16) Information received by a Digital Services Coordinator, the Commission, the Board, or another competent authority that has been granted access to AGORA through AGORA from another Digital Services Coordinator, the Commission, the Board, or another such competent authority should not be deprived of its value as evidence in criminal, civil or administrative proceedings in accordance with relevant EU and national laws solely on the ground that it originated in another Member State, or was received by electronic means, and it should be treated by the relevant AGORA actor in the same way as similar documents originating in its Member State.
- (17) It should be possible to process the name and contact details of AGORA administrators and AGORA users necessary to fulfil the objectives of Regulation (EU) 2022/2065 and of this Regulation, including monitoring of the use of AGORA by AGORA administrators and AGORA users, communication, training and awareness-raising initiatives, and gathering information in connection with the supervision, investigation, enforcement and monitoring of services within the scope of Regulation (EU) 2022/2065, or mutual assistance thereof.
- (18) In order to ensure the effective monitoring of, and reporting on, the functioning of AGORA, the Digital Services Coordinators, the Board and other competent authorities that have been granted access to AGORA should make relevant information available to the Commission.
- (19) Data subjects should be informed about the processing of their personal data in AGORA and the rights they benefit from, in particular the right of access to data relating to them, and the right to have inaccurate data corrected and illegally processed data erased in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.
- (20) Each AGORA actor, as controller with respect to the data processing activities that it performs in connection with the supervision, investigation, enforcement and monitoring of services in scope of Regulation (EU) 2022/2065 should ensure that data subjects can exercise their rights in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725. This should include establishing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

- (21) The implementation of this Regulation and the performance of AGORA should be monitored in the report on the functioning of AGORA based on statistical data from AGORA and any other relevant data. The Commission should submit the report to the European Parliament, the Council and the European Data Protection Supervisor. The performance of the Digital Services Coordinators, the Board and other competent authorities that have been granted access to AGORA should be evaluated, inter alia, based on average reply times with the aim of ensuring efficient and adequate replies. This report should also address aspects relating to the protection of personal data in AGORA, including data security.
- (22) The European Data Protection Supervisor has been consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725, and delivered an opinion on 4 January 2024,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

This Regulation lays down the practical and operational arrangements for the functioning of a reliable and secure information sharing system, hereinafter 'AGORA', for supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.

Article 2

Information sharing system

1. The information sharing system AGORA is hereby established.
2. AGORA is a software application accessible via the Internet, and the tool used for the exchange of information, including, where necessary, personal data, which would otherwise take place via other means, including regular mail or electronic mail.
3. AGORA shall be used for the exchange of information, including the exchange of information containing personal data, between Digital Services Coordinators, the Commission, and the European Board for Digital Services ('the Board'), as well as with other competent authorities that are granted access to AGORA to carry out the tasks conferred upon them in accordance with Regulation (EU) 2022/2065, in relation to the supervision, investigation, enforcement and monitoring of that regulation.

Article 3

Definitions

For the purposes of this Regulation, in addition to the definitions set out in Article 3 and 49(1) of Regulation (EU) 2022/2065, Article 4 of Regulation (EU) 2016/679, and Article 3 of Regulation (EU) 2018/1725, the following definitions shall apply:

- a) 'AGORA' means the information sharing system established and maintained by the Commission to support all communications pursuant to Regulation (EU) 2022/2065 between AGORA actors for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065;
- b) 'AGORA actor' means the Digital Services Coordinators, the Commission, the Board, or other competent authorities that are or may be granted access to AGORA where necessary for them to carry out the tasks conferred on them in accordance with Regulation (EU) 2022/2065;

- c) 'AGORA user' means a natural person working under the authority of an AGORA actor, and registered as such in AGORA, for the purpose of performing the tasks conferred on the AGORA actor by Regulation (EU) 2022/2065;
- d) 'AGORA administrator' means an AGORA user appointed by an AGORA actor for the purpose of managing AGORA for that actor.

CHAPTER II

FUNCTIONS AND RESPONSIBILITIES IN RELATION TO AGORA

Article 4

Responsibilities of the Commission

1. The Commission shall be responsible for carrying out the following tasks in relation to AGORA:
 - (a) providing AGORA in all official Union languages, and maintaining AGORA;
 - (b) ensuring the reliability, security, availability, maintenance and development of the software and IT infrastructure of AGORA;
 - (c) offering automated machine-translation tools for the translation of documents and messages exchanged through AGORA;
 - (d) providing support to other AGORA actors in relation to the use of AGORA;
 - (e) registering at least one AGORA administrator on behalf of each Digital Services Coordinator and of the Board, and granting them access to AGORA;
 - (f) appointing at least one AGORA administrator;
 - (g) performing processing operations on personal data in AGORA, where provided for in this Regulation, for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065;
 - (h) auditing, monitoring, and preparing reports needed for auditing and monitoring of AGORA under Regulation (EU) 2022/2065;
 - (i) providing knowledge, training, and support, including technical assistance, to AGORA administrators;
 - (j) monitoring performance by all other AGORA actors under this Regulation in accordance with Article 15.
2. In order to assist the Commission in the performance of the tasks listed in paragraph 1, the other AGORA actors shall provide the Commission with information relating to operations performed by them in AGORA.

Article 5

Processing of personal data by the Commission

1. The Commission shall be a processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 with respect to the processing of personal data when registering AGORA administrators.
2. The Commission shall be a separate controller within the meaning of Article 3, point (8), of Regulation (EU) 2018/1725 with respect to the processing of personal data of its own AGORA administrators and AGORA users.
3. Where the Commission processes personal data in the operation of AGORA for the purpose of sharing, requesting and accessing information, requesting action and requesting support, it shall be considered a separate controller, within the meaning of Article 3, point (8), of Regulation (EU) 2018/1725, from the other AGORA actors for the personal data processing activities it carries out.

4. Where the Commission processes personal data in the operation of AGORA on behalf of other AGORA actors for the purpose of sharing, requesting and accessing information, requesting action and requesting support, it shall be considered a processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725.
5. For the purposes of this Regulation, the responsibilities of the Commission as processor for data processing activities conducted in AGORA by those other AGORA actors shall be defined in accordance with Annex II.

Article 6

Responsibilities of Digital Services Coordinators

1. Each Digital Services Coordinator shall appoint, for its Member State, at least one AGORA administrator.
2. Each Digital Services Coordinator shall be responsible for ensuring that, in relation to the performance of the tasks conferred on it in accordance with Regulation (EU) 2022/2065, only authorised AGORA users have access to AGORA.
3. Each Digital Services Coordinator shall inform the Commission of the AGORA administrator appointed by it in accordance with paragraph 1 without delay. The Commission shall share that information with the other Digital Services Coordinators and the Board.
4. Each Digital Services Coordinator shall ensure that the responsibilities of the AGORA administrator pursuant to this Regulation are fulfilled.
5. Digital Services Coordinators shall be separate controllers within the meaning of Article 4, point (7), of Regulation (EU) 2016/679 with respect to the processing of personal data when registering their AGORA users and granting them access to AGORA.
6. Where the Digital Services Coordinators process personal data in the operation of AGORA for the purpose of sharing information, requesting and accessing information, answering requests for information, making referrals, requesting action and requesting support, they shall be separate controllers within the meaning of Regulation (EU) 2016/679 for the processing activities they carry out.
7. Where other competent authorities designated by the Member States pursuant to Article 49(1) of Regulation (EU) 2022/2065, which are not the Digital Services Coordinator, process personal data in the operation of AGORA, such authorities shall be separate controllers within the meaning of Regulation (EU) 2016/679.

Article 7

Responsibilities of the Board

1. The Board shall appoint one AGORA administrator. The AGORA administrator shall be part of the administrative and analytical support provided to the Board pursuant to Article 62(4) of Regulation (EU) 2022/2065.
2. The Board shall be responsible for ensuring that only authorised AGORA users have access to AGORA.
3. The Board shall inform the Commission of the identity of its AGORA administrator appointed in accordance with paragraph 1, and of the tasks for which they are responsible under Article 8 of this Regulation, without delay. The Commission shall share this information with the Digital Services Coordinators.

Article 8

Responsibilities of AGORA administrators

AGORA administrators shall be responsible for:

- a) registering AGORA users, and granting and revoking access to AGORA;

- b) acting as the main contact point for the Commission for issues relating to AGORA, including providing information on aspects relating to the protection of personal data in accordance with this Regulation, Regulation (EU) 2016/679, and Regulation (EU) 2018/1725;
- c) providing knowledge, training and support, including technical assistance and a helpdesk, to AGORA users registered by them;
- d) ensuring the efficient provision of adequate responses by AGORA actors.

Article 9

Access rights of AGORA actors

1. AGORA actors shall grant and revoke access rights to AGORA administrators for which they are responsible.
2. Only authorised AGORA administrators and authorised AGORA users shall have access to AGORA.
3. AGORA actors shall put in place appropriate means to ensure that AGORA administrators and AGORA users are allowed to access personal data processed in AGORA only where strictly necessary for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.
4. Where a procedure relating to the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065 involves the processing of personal data, only AGORA administrators and AGORA users participating in that procedure shall have access to such personal data.

Article 10

Confidentiality

1. Each Member State and the Commission shall apply their own rules on professional secrecy or other equivalent duties of confidentiality to their AGORA administrators and AGORA users in accordance with national or Union law.
2. Each AGORA actor shall ensure that demands from other AGORA actors for confidential treatment of information exchanged in AGORA are complied with by AGORA administrators and AGORA users working under their authority.

CHAPTER III

PROCESSING OF PERSONAL DATA AND SECURITY

Article 11

Processing of personal data in AGORA

1. The transmission, storage and other processing of personal data in AGORA may take place only as necessary and proportionate and only for the following purposes:
 - (a) supporting communications between AGORA actors in connection with the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065;
 - (b) case-handling by AGORA actors when carrying out their own activities in connection with the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065;
 - (c) performing the business and technical transformations of data listed in this Regulation, where this is necessary to enable the exchange of information referred to in points (a) and (b).

2. The processing of personal data may take place in AGORA only in respect of the following categories of data subjects:
 - (a) natural persons whose personal information is contained in documents obtained in connection with the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065;
 - (b) AGORA administrators and AGORA users that have been granted access to AGORA.
3. The processing of personal data may take place in AGORA only in respect of the following categories of personal data:
 - a) identification data, contact details, case involvement data, case related data, and any other information deemed necessary for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065;
 - b) name, address, contact information, contact number and user ID of the AGORA administrators and AGORA users referred to in paragraph 2, point (b).
4. AGORA shall store the categories of personal data listed under Article 11(3) of this Regulation and the logs indicating information about the flow and movements of the exchanged data carried out for the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.
5. The storage of data referred to in paragraph 2 shall be performed using information technology infrastructure located in the European Economic Area.
6. Each AGORA actor shall ensure that data subjects can exercise their rights in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725, and shall be responsible for compliance with these regulations for the personal data processing activities carried out on its behalf.
7. The national Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of their respective competence, shall ensure coordinated supervision of AGORA and its use by AGORA administrators and AGORA users.

Article 12

Joint controllership in AGORA

1. The Digital Services Coordinators shall be joint controllers pursuant to Article 26(1) of Regulation (EU) 2016/679 for the transmission, storage and other processing of personal data in AGORA in respect of the activities of the Board carried out in the context of the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.
2. When joint investigations are carried out pursuant to Article 60 of Regulation (EU) 2022/2065 in the context of the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065, the concerned Digital Services Coordinators shall be joint controllers, within the meaning of Article 26(1) of Regulation (EU) 2016/679, for the transmission, storage and other processing of personal data in AGORA in the context of a particular joint investigation.
3. For the purposes of paragraphs 1 and 2, responsibilities shall be allocated among joint controllers in accordance with Annex I.
4. The Commission shall be a processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 for the processing of personal data carried out on behalf of the Digital Services Coordinators for the purpose of the activities of the Board, and for joint investigations pursuant to Article 60 of Regulation (EU) 2022/2065 carried out in the context of the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.

*Article 13***Security**

1. The Commission shall put in place the necessary, state-of-the-art measures to ensure security of personal data processed in AGORA, including appropriate data access control and a security plan, which shall be kept up-to-date.
2. The Commission shall put in place the necessary, state-of-the-art measures in the event of a security incident, take remedial action, and ensure that it shall be possible to verify what personal data have been processed in AGORA, when, by whom, and for what purpose.

CHAPTER IV

FINAL PROVISIONS*Article 14***Translation**

1. The Commission shall make AGORA available in all official languages of the Union, and offer to AGORA users automated machine-translation tools for the translation of documents and messages exchanged in AGORA.
2. A Digital Services Coordinator or any other competent authority to which access to AGORA is granted may produce, in relation to the performance of any of the tasks conferred on it in accordance with Regulation (EU) 2022/2065, any information, document, finding, statement, or certified true copy which it has received in AGORA, on the same basis as similar information obtained in its own country, for purposes compatible with those for which the data were originally collected and in accordance with relevant EU and national laws.

*Article 15***Monitoring and reporting**

1. The Commission shall regularly monitor the functioning of AGORA and shall regularly evaluate its performance.
2. By 17 February 2027, and every three years thereafter, the Commission shall submit to the European Parliament, the Council and the European Data Protection Supervisor a report on the implementation of this Regulation. The report shall include information on the monitoring and evaluation carried out in accordance with paragraph 1, and on the performance of AGORA actors in connection with AGORA with a view to ensuring efficient information sharing and adequate replies. The report shall also address aspects of implementation relating to the protection of personal data in AGORA, including data security.
3. For the purpose of producing the report referred to in paragraph 2, the Digital Services Coordinators, the Board and other competent authorities to which access is granted where necessary to carry out the tasks conferred to them in accordance with Regulation (EU) 2022/2065 shall, on an annual basis, provide the Commission with any information relevant to the application of this Regulation in the form of reports, including on the application of the data protection requirements and data security laid down in it.

*Article 16***Costs**

1. The costs incurred for the set-up, maintenance and operation of AGORA shall be covered by the annual supervisory fees collected by the Commission in accordance with Article 43(2) of Regulation (EU) 2022/2065 and Commission Delegated Regulation (EU) 2023/1127 ⁽⁴⁾.
2. The costs for AGORA operations at Member State level, including the human resources needed for training, promotion, technical assistance and helpdesk activities, as well as for the administration of AGORA at national level and any adaptations required to national networks and information systems shall be borne by the Member State which incurs them.

*Article 17***Effective application**

The Member States shall take all necessary measures to ensure effective application of this Regulation by their AGORA actors.

*Article 18***Entry into force**

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

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

Done at Brussels, 15 February 2024.

For the Commission
The President
Ursula VON DER LEYEN

⁽⁴⁾ Commission Delegated Regulation (EU) 2023/1127 of 2 March 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of very large online platforms and very large online search engines (OJ L 149, 02.03.2023, p. 16, ELI: http://data.europa.eu/eli/reg_del/2023/1127/oj).

ANNEX I

Responsibilities of the Digital Services Coordinators as joint controllers for data processing activities conducted in the context of AGORA for joint investigations and for the activities of the Board**SECTION 1***Subsection 1***Scope of the joint controllership arrangement**

- (1) The following joint controllership arrangement shall apply to the concerned Digital Services Coordinators when conducting joint investigations pursuant to Article 60 of Regulation (EU) 2022/2065.
- (2) The following joint controllership arrangement shall apply to the Digital Services Coordinators as members of the Board for the processing of personal data activities of the Board pursuant to Regulation (EU) 2022/2065, carried out in the context of the supervision, investigation, enforcement and monitoring of services in scope of Regulation (EU) 2022/2065.

*Subsection 2***Allocation of responsibilities**

- (1) The joint controllers shall process personal data through AGORA.
- (2) The Digital Services Coordinators shall remain the sole controllers for the collection, use, disclosure and any other processing of personal data carried out outside AGORA. The Digital Services Coordinators shall also remain the sole controllers for the personal data processing activities they carry out within AGORA for the supervision, investigation, enforcement and monitoring of services in scope of Regulation (EU) 2022/2065.
- (3) Each joint controller shall be responsible for the processing of personal data in AGORA in accordance with Articles 5, 24 and 26 of Regulation (EU) 2016/679.
- (4) Each joint controller shall set up a contact point with a functional mailbox for the communication between the joint controllers themselves and between the joint controllers and the processor.
- (5) Each joint controller, when so requested, shall provide a swift and efficient assistance to the other joint controllers in execution of this arrangement, while complying with all applicable requirements of Regulation (EU) 2016/679 and other applicable data protection rules, including obligations towards its own respective supervisory authority.
- (6) The joint controllers shall define the working modalities through which processing of personal data through AGORA shall take place, and shall provide agreed upon instructions to the Commission as a processor.
- (7) Instructions to the processor shall be sent by any of the joint controllers' contact points in agreement with the other joint controllers. The joint controller who provides the instruction shall provide them to the processor in writing and inform all other joint controllers of this. If the matter at hand is sufficiently time-critical that it does not allow for a meeting of the joint controllers, an instruction may be provided nonetheless, but may be rescinded by the joint controllers. This instruction shall be given in writing, and all other joint controllers shall be informed of this at the time of giving the instruction.
- (8) The working modalities between joint controllers shall not preclude any of the joint controllers' individual competence to inform their competent Supervisory Authority in accordance with Articles 24 and 33 of Regulation (EU) 2016/679. Such notification shall not require the consent of any of the other joint controllers.

- (9) The working modalities between joint controllers shall not preclude any of the joint controllers to cooperate with its respective competent Supervisory Authority established under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.
- (10) Only persons authorised by each joint controller shall access the personal data exchanged.
- (11) Each joint controller shall maintain a record of the processing activities under its responsibility. The joint controllership shall be indicated in such a record.

Subsection 3

Responsibilities and roles for handling requests of and informing data subjects

- (1) Each controller shall provide information to natural persons whose data is being processed for joint investigations and activities of the Board carried out in the context of supervision, investigation, enforcement and monitoring of services in scope of Regulation (EU) 2022/2065, in accordance with Article 14 of Regulation (EU) 2016/679, unless this would prove impossible or would involve a disproportionate effort.
- (2) Each controller shall act as the contact point for natural persons whose personal data it has processed and shall handle the requests submitted by data subjects or their representatives in the exercise of their rights in accordance with Regulation (EU) 2016/679. If a joint controller receives a request from a data subject that relates to the processing by another joint controller, it shall inform the data subject of the identity and contact details of the responsible joint controller. If requested by another joint controller, the joint controllers shall assist each other in handling data subjects' requests and shall reply to each other without undue delay and at the latest within one month from receiving a request for assistance.
- (3) Each controller shall make available the content of this Annex to data subjects.

SECTION 2

MANAGEMENT OF SECURITY INCIDENTS, INCLUDING PERSONAL DATA BREACHES

- (1) The joint controllers shall assist each other in the identification and handling of any security incidents, including personal data breaches, linked to the processing in AGORA.
- (2) In particular, the joint controllers shall notify each other of:
 - (a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing processing in AGORA;
 - (b) any personal data breach, the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and to mitigate the risk to the rights and freedoms of natural persons; and
 - (c) any breach of the technical and/or organisational safeguards of the processing operation in AGORA.
- (3) The joint controllers shall communicate any personal data breaches related to the processing operation in AGORA to the Commission, to the competent data protection supervisory authorities and, where required, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679, or following notification by the Commission.
- (4) Each controller shall implement appropriate technical and organisational measures, designed to:
 - (a) ensure and protect the availability, integrity and confidentiality of the personal data jointly processed;
 - (b) protect against any unauthorised or unlawful processing, loss, use, disclosure or acquisition of or access to any personal data in its possession; and
 - (c) ensure that access to the personal data is not disclosed or granted to anyone else other than the recipients or processor.

SECTION 3

DATA PROTECTION IMPACT ASSESSMENT

If a controller, in order to comply with its obligations under Articles 35 and 36 of Regulation (EU) 2016/679 needs information from another controller or from the processor, it shall send a specific request to the functional mailbox referred to in Subsection 2(4) of Section 1. The latter shall use its best efforts to provide any such information.

ANNEX II

Responsibilities of the commission as processor for data processing activities conducted in the context of AGORA by Digital Services Coordinators, other national authorities and the Board

- (1) The Commission shall:
 - (a) set up and ensure a secure and reliable communication infrastructure, the AGORA, on behalf of the Digital Services Coordinators, other national authorities and the Board that supports the exchange of information for coordinated investigations, consistency mechanisms and activities of the Board, and
 - (b) process personal data only based on documented instructions from the controllers and joint controllers, unless required to do so under Union or Member State laws; in such a case, the Commission shall inform the controllers and joint controllers of that legal requirement before carrying on the processing activity, unless that law prohibits submitting such information on important grounds of public interest.
- (2) To fulfil its obligations as processor for the Digital Services Coordinators, other national authorities and the Board, the Commission may use third parties as sub-processors. If it is the case, the controllers and joint controllers shall authorise the Commission to use sub-processors or replace sub-processors where necessary. The Commission shall inform the controllers and joint controllers of said use or replacement of sub-processors, thereby giving the controllers and joint controllers the opportunity to object to any such changes. The Commission shall ensure that the same data protection obligations as set out in this Regulation apply to these sub-processors.
- (3) The processing by the Commission shall entail:
 - (a) authentication and access control with regard to all AGORA administrators and AGORA users;
 - (b) authorisation of AGORA administrators and AGORA users to create, update and delete any records and information contained in AGORA;
 - (c) reception of the personal data referred to in Article 12(3) of this Regulation uploaded by national AGORA users and AGORA administrators by providing an application programming interface that allows national AGORA users and AGORA administrators to upload the relevant data;
 - (d) storage of the personal data in AGORA;
 - (e) making the personal data available for access and download by AGORA administrators and AGORA users and any other necessary data processing activity;
 - (f) deletion of the personal data at their expiration date or upon instruction of the controller that submitted them;
 - (g) after the end of the provision of service, deletion of any remaining personal data unless Union or Member State laws require storage of such personal data.
- (4) The Commission shall take all state of the art organisational, physical, and logical security measures to ensure AGORA functioning. To this end, the Commission shall:
 - (a) designate a responsible entity for the security management of AGORA, communicate to the joint controllers its contact information and ensure its availability to react to security threats;
 - (b) assume the responsibility for the security of AGORA, including regularly carrying out tests, evaluations and assessments of the security measures;
 - (c) ensure that AGORA administrators and AGORA users that are granted access to AGORA are subject to a contractual, professional or statutory obligation of confidentiality.
- (5) The Commission shall take all necessary security measures to avoid compromising the smooth operational functioning of AGORA. This shall include:
 - (a) risk assessment procedures to identify and estimate potential threats to AGORA;
 - (b) audit and review procedure to:
 - check the correspondence between the implemented security measures and the applicable security policy;

- control on a regular basis the integrity of AGORA files, security parameters and granted authorisations;
 - detect security breaches and intrusions into AGORA;
 - implement changes to mitigate existing security weaknesses in AGORA;
 - define the conditions under which to authorise, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures subject to conditions that respect Protocol (No 7) to the Treaty on the Functioning of the European Union on the Privileges and Immunities of the European Union;
- (c) changing the control procedure to document, measure the impact of a change before its implementation, and keep the controllers and joint controllers informed of any changes that can affect the communication with and/or the security of AGORA;
- (d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of AGORA equipment is to be performed;
- (e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers affected, inform without delay the controllers for them to notify the national data protection supervisory authorities of any personal data breach and define a disciplinary process to deal with security breaches in AGORA.
- (6) The Commission shall take state of the art physical and logical security measures for the facilities hosting AGORA and for the controls of data and security access thereto. To this end, the Commission shall:
- (a) enforce physical security to establish distinct security perimeters and allowing detection of breaches in AGORA;
 - (b) control access to AGORA facilities and maintain a AGORA visitor register for tracing purposes;
 - (c) ensure that external individuals granted access to the premises are escorted by duly authorised staff;
 - (d) ensure that equipment cannot be added, replaced or removed without prior authorisation from the designated responsible bodies;
 - (e) control access from and to the AGORA;
 - (f) ensure that AGORA administrators and AGORA users who access AGORA are identified and authenticated;
 - (g) review the authorisation rights related to the access to AGORA in case of a security breach affecting AGORA;
 - (h) keep the integrity of the information transmitted through AGORA;
 - (i) implement technical and organisational security measures to prevent unauthorised access to personal data in AGORA;
 - (j) implement, whenever necessary, measures to block unauthorised access to AGORA (i.e., block a location/IP address).
- (7) The Commission shall:
- (a) take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality and security;
 - (b) maintain a risk management plan related to its area of responsibility;
 - (c) monitor, in real time, the performance of all the service components of AGORA, produce regular statistics and keep records;
 - (d) provide support for AGORA in English to AGORA administrators and AGORA users;
 - (e) assist the controllers and joint controllers by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of Regulation (EU) 2016/679;

- (f) support the controllers and joint controllers by providing information concerning AGORA to implement the obligations pursuant to Articles 32, 33, 34, 35 and 36 of Regulation (EU) 2016/679;
 - (g) ensure that data processed within AGORA is unintelligible to any person who is not authorised to access it;
 - (h) take all relevant measures to prevent unauthorised access to transmitted personal data via AGORA;
 - (i) take measures in order to facilitate communication between the controllers and joint controllers;
 - (j) maintain a record of processing activities carried out on behalf of the controllers and joint controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.
-