DECISION OF THE MANAGEMENT BOARD

Adopting implementing rules relating 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

The Management Board of the European Securities and Markets Authority (ESMA)

Having regard to the Treaty on the Functioning of the European Union[1],

Having regard to 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 [2](the "Regulation" and "ESMA"), and in particular Article 71 thereof

Having regard to Regulation (EU) 2018/1725, and in particular Article 45(3) thereof.[3]

Whereas:

(1) Regulation (EU) 2018/1725 (European Data Protection Regulation - EDPR) lays down data protection principles and rules applicable to all Union Institutions and bodies and repeals Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;

(2) Regulation (EU) 2016/679 lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union and it stresses the need to introduce necessary adaptations of Regulation (EC) No 45/2001 in order to provide a strong and coherent data protection framework within the Union;

---

[1] OJ C 115, 9.5.2008, p.47.
[2] OJ L 331, 15.12.2010, p. 84.
[3] OJ L 295, 21.11.2018, p. 39–98

(3) In line with Article 25 of the EDPR, ESMA has the possibility to impose restrictions on data subjects rights as set up in Articles 14 to 22, 35 and 36 as well as Article 4 of the EDPR. To that effect, ESMA may be obliged to defer the information to data subjects and other data subjects' rights to protect, in particular, its own investigations and procedures, the investigations and proceedings of other public authorities, as well as the rights of other persons related to its investigations and procedures;

(4) ESMA as controller within the meaning of Article 3(8) of the EDPR is responsible for determining the purposes and the means of the processing of personal data by complying with the requirements of the EDPR.

(5) The tasks and the duties of the controller may be, individually or jointly, delegated by the Executive Director to senior ESMA staff members unless the performance of such tasks would create a possible conflict of interests with their roles or duties.

(6) According to Article 31 of the EDPR, the EU institutions have an obligation to maintain their records of processing activities in a central register and to make such register publicly accessible. The central register is an important tool to ensure accountability and transparency regarding processing operations.

(7) Pursuant to Article 45(3) of the EDPR further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer (DPO) to be appointed by each Union institution or body. The purpose of the implementing rules is also to lay down procedures which will enable data subjects to exercise their rights and all persons within the Union institutions or bodies who are involved in the processing of personal data to fulfil their obligations.

(8) This Decision should repeal the previous Decision of the Management Board on Implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (as amended) dated 11 April 2011 (ESMA/2011/MB/57)

Has adopted this decision:

SECTION 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Decision lays down the general rules implementing the EDPR as regards ESMA. In particular, it supplements the provisions set out in the EDPR relating to the DPO's appointment and status, as well as to his/her tasks, duties and powers.

2. This Decision also clarifies the roles, tasks and duties of controller and implements the rules pursuant to which data subjects may exercise their rights.

Article 2

Definitions

1. For the purposes of this Decision, and without prejudice to the definitions in the EDPR, the following definitions shall apply:

    a) 'data subject' shall mean an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

    b) 'controller' means ESMA, as the legal entity responsible for the processing operation, represented by the Executive Director.

    c) 'joint controller' means any Union institution and body or any public institution or entity other than Union institutions and bodies with which ESMA jointly determines the purposes and the means of processing of personal data.

    d) 'internal data controllers' means the senior persons to whom the tasks and the duties of the controller may be individually or jointly delegated by the Executive Director.

    e) 'data controllers' means the Executive Director, acting in his/her capacity as controller and the internal data controllers.

SECTION 2

THE DATA PROTECTION OFFICER

Article 3

Appointment, statute and independence

1. The Executive Director shall appoint the DPO from amongst ESMA's staff graded equal or superior to AD7 or equivalent on the basis of his or her professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 45 of the EDPR. The DPO shall report to the Executive Director in the performance of his or her duties as Data Protection Officer.

2. The Executive Director shall register the DPO with the European Data Protection Supervisor.

3. The DPO may perform other duties, provided that they do not result in a conflict of interests with the role of Data Protection Officer, particularly in relation to the application of the provisions laid down in the EDPR.

4. The DPO shall be appointed for a period of three years renewable.

5. The DPO may be dismissed from his or her post only with the consent of the European Data Protection Supervisor and only if he or she no longer fulfils the conditions required for the performance of his or her duties. The European Data Protection Supervisor shall be consulted in writing and a copy sent to the Data Protection Officer.

6. The DPO shall be independent in the performance of his or her duties. In that regard, he or she may not receive any instructions, in particular from the Executive Director or any other source as regards the internal application of the provisions laid down in the EDPR or his or her cooperation with the European Data Protection Supervisor. The DPO shall refrain from any act which is incompatible with the nature of his or her duties.

7. The DPO shall maintain, including once he or she has ceased his or her duties, professional secrecy as regards any confidential documents or information which he or she obtains in the course of his or her duties.

Article 4

Resources

1. The Executive Director shall ensure that the DPO has adequate time and resources, including training, to carry out his or her duties.

2. The DPO may be assisted in his or her day-to-day activities by an assistant.

3. The DPO may delegate his or her tasks and be represented (in his or her absence or when otherwise engaged) by one or more deputies, as necessary. The provisions on independence in Article 3(5) of this Decision apply to the deputies.

Article 5

Duties

1. The DPO shall inform and advise the data controllers and the employees who process personal data as part of their functions at ESMA on the application of the provisions laid down in the EDPR. He or she shall carry out his or her tasks in cooperation with the European Data Protection Supervisor.

2. The DPO may be consulted at any time by any person and in particular by data subjects in respect of any matter relating to the application of the EDPR.

3. The DPO shall represent ESMA in respect of any matter relating to data protection. He or she may in particular attend meetings of committees or relevant bodies at international level.

4. The DPO shall not suffer any prejudice on account of the performance of his or her duties.

Article 6

Tasks

The DPO's tasks shall be as follows:

(a) *Provision of information, advice:* the DPO shall inform/advise ESMA's data controllers on the legislation in force, current procedures and existing records. In particular, the DPO shall assist the data controllers in the drafting of Data Protection Impact Assessments and submissions for prior consultations of the European Data Protection Supervisor in line with Article 39 and Article 40 of the EDPR as well as in responding to the requests submitted by the data subjects.

(b) *Assistance in the notification of a personal data breach*: the DPO shall assist the Executive Director acting as controller in the notification of a personal data breach to the European Data Protection Supervisor in accordance with Article 34 of the EDPR.

(c) *Cooperation with the European Data Protection Supervisor:* within his or her area of responsibility, the Officer shall cooperate with the European Supervisor at the latter's request or on his or her own initiative, particularly as regards dealing with complaints and carrying out inspections. The DPO shall inform the European Supervisor regarding any significant development at ESMA which has a bearing on the protection of personal data.

(d) *Publication of a central register of records:* the DPO shall, pursuant to Article 31 of the EDPR, ensure that the central register of the records of processing activities maintained by the data controllers is publicly available.

(e) *Data subject rights:* the DPO shall ensure that processing operations do not undermine the rights and freedoms of data subjects without any legal basis for restricting those rights, and that no person suffers loss or damage for having brought to the Data Protection Officer's attention a matter which in the view of that person constitutes an infringement of the EDPR. The DPO shall ensure that rights and obligations of data subject rights are easily accessible on ESMA's website.

Article 7

Powers

1. In order to perform his or her tasks and in accordance with the conditions laid down in the EDPR, the DPO may:

(a) on his or her own initiative, make recommendations to the data controllers or to the Executive Director on issues concerning the application of the provisions relating to data protection or included in these implementing rules;

(b) investigate issues and facts (on his or her own initiative or at the request of controller, ESMA's Staff Committee or any individual) which relate directly to his or her powers and responsibilities and which have been brought to his or her knowledge. He or she shall consider them in accordance with the principle of impartiality and with due regard to the rights of the data subject. The Data Protection Officer shall forward his or her findings to the person who submitted the request and to the controller;

(c) report any breach of the provisions laid down in the EDPR to the Executive Director;

(d) regularly attend meetings with the European Data Protection Supervisor and/or the Data Protection Officers of the other institutions and bodies with a view to

establishing a mutual exchange of information, engaging in interinstitutional cooperation and harmonising the application of the procedures in force;

(e) issue an opinion on the lawfulness of actual or proposed processing operations, on the measures required in order to ensure that such operations are lawful and on the suitability or inadequacy of data or of security measures, if necessary. The opinion may in particular relate to any issue concerning the notification of data-processing operations.

2. In performing his or her duties, the DPO:

(a) shall have access at any time to data being processed, to all premises, all data processing installations and all information media;

(b) may, without prejudice to the duties and powers of the European Data Protection Supervisor, propose administrative measures to the Executive Director and make general recommendations on the appropriate application of the EDPR;

(c) may, in particular circumstances, make any other recommendation to the Executive Director and/or all the other parties concerned for the concrete improvement of data protection;

(d) may bring to the attention of the Executive Director and the human resources service any failure by a staff member to comply with the obligations pursuant to the EDPR; and

(e) may request an opinion from the relevant areas of ESMA on any issue associated with his or her tasks and duties.

3. No-one shall suffer prejudice on account of bringing a matter to the DPO's attention alleging a breach of the provisions of the EDPR.

4. ESMA staff shall cooperate with the DPO in the performance of his or her duties, in particular for the conduct of investigations referred to in point 1 (b) above, without requiring further authorisation.

SECTION 3

DATA CONTROLLERS

Article 8

Tasks and duties of the data controllers

1. The data controllers shall ensure that all processing operations involving personal data that are performed within their area of responsibility comply with the EDPR and any other Union data protection provisions.

2. The tasks and the duties of the controller may be delegated by the Executive Director to senior ESMA Staff members unless the performance of such tasks would create a possible conflict of interests with their roles or duties.

3. The data controllers shall ensure that the DPO is kept informed without undue delay:

   (a) when an issue arises that has, or might have, data protection implications;

   (b) before the adoption of any opinion, document, internal policies or internal decision that may have an impact on ESMA's data protection compliance.

   (c) when a data subject directly exercises his/her rights vis-à-vis the controller or internal data controllers in line with Article 11 of this Decision;

   (d) in case of a personal data breach or other incident;

   (e) about contacts with external parties with relevance to the application of EDPR and any direct interaction of the controller and any internal data controller with the European Data Protection Supervisor.

   (a) The data controllers shall in particular: ensure that the relevant processing operations relating to personal data are identified in a timely manner;

   (b) promote and raise awareness of the guidance provided by the DPO and the European Data Protection Supervisor;

   (c) consult the DPO in a timely manner on any activities related to the processing of personal data and in any case well before the processing of personal data starts;

   (d) conduct data protection impact assessments in cooperation with the DPO and pursuant to the provisions of Article 39 of the EDPR.

   (e) make sure that the activity of any processor complies with the relevant requirements set out in EDPR;

   (f) comply with any relevant internal policies related to the processing of personal data or any other data protection issues;

   (g) identify, with the assistance of the DPO, any possible personal data breach to be internally reported to the Executive Director acting as controller;

(h) maintain and keep regularly updated records of processing activities in accordance with Article 31 of EDPR, using as a rule the template approved and provided by the DPO;

4. The Executive Director acting as controller shall notify a personal data breach to the European Data Protection Supervisor pursuant to Article 34 of the EDPR.

5. When assisting the DPO and the European Data Protection Supervisor in the performance of their duties, the data controllers shall provide full information to them, grant access to personal data and respond to questions in a timely manner.

Article 9

Central register

1. The data controllers shall submit their records of processing operations pursuant to Article 31 of the EDPR to the DPO. The DPO shall keep and manage the central register of records of processing activities.

2. The central register shall serve as a repository of the personal data processing operations conducted at the ESMA. It shall provide information to data subjects and facilitate the exercise of their rights in line with Articles 17 to 24 of the EDPR. The central register shall be made public. The central register shall contain at least the information referred to in Article 31(1)(a) to (g) of the EDPR.

Article 10

Joint controllers

1. In the exercise of its mandate, ESMA may act as joint controller together with one or more controllers as set forth in Article 28 of the EDPR.

2. In case ESMA acts as joint controller with one or more Union institutions or bodies, or institutions or bodies of Member States, the responsibilities of the joint controllers for compliance with data protection obligations shall be established in Union law.

3. In case ESMA acts as joint controller with national competent authorities, the responsibilities of joint controllers for compliance with data protection obligations may be established by Union law or by further legal instruments.

4. In case ESMA acts as joint controller with one or more controllers which are private commercial entities, the responsibilities of the joint controllers for compliance with data

protection obligations shall be established in contractual arrangements entered into between the joint controllers.

SECTION 4

DATA SUBJECT'S RIGHTS

Article 11

Exercise of data subjects' rights

1. Data subjects shall have the right to approach the controller or any relevant internal data controller to exercise their rights pursuant to Articles 17 to 24 of the EDPR, as specified below.

2. Data subjects' rights may only be exercised by the data subject or his/her duly authorised representative. Such persons may exercise any of these rights free of charge.

3. Requests to exercise data subjects' rights shall be submitted in writing or where appropriate, by electronic means. Upon receipt of a request from the data subject, the controller or internal data controller concerned shall within 14 days send an acknowledgment of receipt of the request to the data subject and inform him/her about the possibility to lodge a complaint with the European Data Protection Supervisor and the possibility to seek judicial redress.

4. If the controller or internal data controller concerned has reasonable doubts concerning the identity of the natural person or their authorised representative, he or she may request the provision of additional information allowing identification of the data subject. Where applicable, the controller or concerned internal data controller shall check the relevant authorisation if the data subject is represented by an authorised representative. Further information may be requested from the data subject, to allow a targeted response reaction to the request.

5. In accordance with Article 14(3) and 14(4) of the EDPR, the controller or internal data controller concerned shall provide information to the data subject on action taken in relation to a request without undue delay and at the latest within one month of receipt of the request. If necessary, this period may be extended by two further months, taking into account the complexity and number of data subjects' requests. The data subject shall be informed of any extensions within one month of receipt of the request and state the reasons for the delay.

6. The controller or internal data controller concerned shall respond to the data subject's request in writing, if appropriate, and in case the data subject has made a request by

electronic means, he or she shall also provide the requested information in a commonly used electronic format.

7. The data subject may at any point contact the DPO, in particular:

   (a) if the controller or internal data controller concerned does not respect the above-mentioned time limits,

   (b) when he/she is dissatisfied with the action taken by the controller or internal data controller concerned or

   (c) if he/she wishes to lodge a complaint with the European Data Protection Supervisor.

8. In the event of manifest abuse of the exercise of the data subjects' rights, for example if such exercise is repetitive, abusive and/ or pointless, the DPO may inform the data subject that the request will not be pursued.

Article 12

Monitoring procedure

1. The data controllers shall assist the Data Protection Officer in the performance of his or her duties and provide him or her with any information which he or she requests within 20 working days. In performing his or her duties, the Data Protection Officer shall have access at all times to the data being processed and to all offices, data-processing installations and data carriers.

2. The Data Protection Officer may decide to carry out any other type of monitoring at any time in order to ensure that the EDPR is being properly applied by ESMA.

Article 13

Exemptions and restrictions

1. Legal acts adopted on the basis of the Treaties or, in matters relating to the tasks of ESMA as laid down in Union law, internal rules laid down by the latter may restrict the application of the Articles referred to in Article 25 of the EDPR on the grounds, and in accordance with the conditions, set out in therein.

2. The internal rules referred to in paragraph 1 shall be clear and precise acts of general application, intended to produce legal effects vis-à-vis data subjects, adopted by the

Management Board of ESMA and subject to publication in the Official Journal of the European Union. The European Data Protection Supervisor shall be consulted prior to the adoption of internal rules as referred to in paragraph 1.

Article 14

Remedies

1. Any person employed by ESMA may lodge a complaint in accordance with Chapter VIII of EDPR.[4]

2. If any person employed by ESMA lodges with the Appointing Authority a complaint pursuant to Article 90 of the Staff Regulations in respect of a matter relating to the processing of personal data, the DPO shall be consulted.

Article 15

Access to documents

Documents produced in the context of these implementing rules shall be subject to Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents as implemented by ESMA.

Article 16

Final provisions

The Executive Director may adopt measures necessary for implementation of this Decision, having regard to the professional standards for DPO issued by the Network of Data Protection Officers of the EU institutions and bodies and any guidelines issued by the European Data Protection Supervisor.

SECTION 5

[4] ESMA staff may also lodge with the Appointing Authority a complaint pursuant to Article 90 of the Staff Regulations in respect of a matter relating to the processing of personal data. Lodging such a complaint does not have the effect of stopping time running for the purposes of lodging a complaint pursuant to Article 90 of the Staff Regulations.

ENTRY INTO FORCE

Article 17

Final provision

This decision enters into force on 29 January 2019.

Done at Paris on 29 January 2019

For the Management Board

The Chair

[SIGNED]

STEVEN MAIJOOR