



DECISION No MB/2019/10
OF THE MANAGEMENT BOARD OF
THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of ENISA

THE MANAGEMENT BOARD OF ENISA

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

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⁽¹⁾ (‘Regulation (EU) 2018/1725’), and in particular Article 25 thereof,

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), and in particular to Article 15(1) thereof,

Having regard to the opinion of the EDPS of 17 October 2019 and to the EDPS Guidance on Article 25 of the Regulation (EU) 2018/1725 and internal rules.

Whereas:

(1) In accordance with Article 25(1) of Regulation (EU) 2018/1725 restrictions of the application of Articles 14 to 22, 35 and 36, as well as Article 4 of that Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22 should be based on internal rules to be adopted by ENISA, where these are not based on legal acts adopted on the basis of the Treaties.

(2) These internal rules, including its provisions on the assessment of the necessity and proportionality of a restriction, should not apply where a legal act adopted

⁽¹⁾ OJ L 295, 21.11.2018, p. 39

on the basis of the Treaties provides for a restriction of data subject rights.

- (3) Where ENISA performs its duties with respect to data subject's rights under Regulation (EU) 2018/1725, it shall consider whether any of the exemptions laid down in that Regulation apply.
- (4) Within the framework of its administrative functioning, ENISA may conduct administrative inquiries, disciplinary proceedings, carry out preliminary activities related to cases of potential irregularities reported to OLAF, process whistleblowing cases, process (formal and informal) procedures of harassment, process internal and external complaints, conduct internal audits, conduct assessments of cybersecurity incidents pursuant to Article 7(4) of the Regulation (EU) 2019/881, carry out investigations by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and internal (IT) security investigations.

ENISA processes several categories of personal data, including hard data ('objective' data such as identification data, contact data, professional data, administrative details, data received from specific sources, electronic communications and traffic data) and/or soft data ('subjective' data related to the case such as reasoning, behavioural data, appraisals, performance and conduct data and data related to or brought forward in connection with the subject matter of the procedure or activity).

- (5) ENISA, represented by its Executive Director, acts as the data controller irrespective of further delegations of the controller role within ENISA to reflect operational responsibilities for specific personal data processing operations.
- (6) The personal data are stored securely in an electronic environment or on paper preventing unlawful access or transfer of data to persons who do not have a need to know. The personal data processed are retained for no longer than necessary and appropriate for the purposes for which the data are processed for the period specified in the data protection notices, privacy statements or records of ENISA.
- (7) The internal rules should apply to all processing operations carried out by ENISA in the performance of administrative inquiries, disciplinary proceedings, preliminary activities related to cases of potential irregularities reported to OLAF, whistleblowing procedures, (formal and informal) procedures for cases of harassment, processing internal and external complaints, internal audits, assessments of cybersecurity incidents pursuant to Article 7(4) of the Regulation (EU) 2019/881, the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725, (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

- (8) They should apply to processing operations carried out prior to the opening of the procedures referred to above, during these procedures and during the monitoring of the follow-up to the outcome of these procedures. It should also include assistance and cooperation provided by ENISA to national authorities and international organisations outside of its administrative investigations.
- (9) In the cases where these internal rules apply, ENISA has to give justifications explaining why the restrictions are strictly necessary and proportionate in a democratic society and respect the essence of the fundamental rights and freedoms.
- (10) Within this framework, ENISA is bound to respect, to the maximum extent possible, the fundamental rights of the data subjects during the above procedures, in particular, those relating to the right of provision of information, access and rectification, right to erasure, restriction of processing, right of communication of a personal data breach to the data subject or confidentiality of communication as enshrined in Regulation (EU) No 2018/1725.
- (11) However, ENISA may be obliged to restrict the information to data subject and other data subject's rights to protect, in particular, its own investigations, the investigations and proceedings of other public authorities, as well as the rights of other persons related to its investigations or other procedures.
- (12) ENISA may thus restrict the information for the purpose of protecting the investigation and the fundamental rights and freedoms of other data subjects.
- (13) ENISA should periodically monitor that the conditions that justify the restriction apply and lift the restriction as far as they do no longer apply.
- (14) The Controller should inform the Data Protection Officer at the moment of deferral and during the revisions.
- (15) Due to the importance of the internal rules for the protection of data subject's rights, the Decision should enter into force as soon as possible after its publication in the Official Journal of the European Union.

HAS ADOPTED THIS DECISION:

Article 1

Subject-matter and scope

1. This Decision lays down rules relating to the conditions under which ENISA in the framework of its procedures set out paragraph 2 may restrict the application

of the rights enshrined in Articles 14 to 21, 35 and 36, as well as Article 4 thereof, following Article 25 of the Regulation (EU) No 2018/1725.

2. Within the framework of the administrative functioning of ENISA, this Decision applies to the processing operations on personal data by ENISA for the purposes of: conducting administrative inquiries, disciplinary proceedings, preliminary activities related to cases of potential irregularities reported to OLAF, processing whistleblowing cases, (formal and informal) procedures of harassment, processing internal and external complaints, conducting internal audits, conducting assessments of cybersecurity incidents pursuant to Article 7(4) of the Regulation (EU) 2019/881, investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

3. The categories of data concerned are hard data (‘objective’ data such as identification data, contact data, professional data, administrative details, data received from specific sources, electronic communications and traffic data) and/or soft data (‘subjective’ data related to the case such as reasoning, behavioural data, appraisals, performance and conduct data and data related to or brought forward in connection with the subject matter of the procedure or activity).

4. Where ENISA performs its duties with respect to data subject’s rights under Regulation (EU) 2018/1725, it shall consider whether any of the exemptions laid down in that Regulation apply.

5. Subject to the conditions set out in this Decision, the restrictions may apply to the following rights: provision of information to data subjects, right of access, rectification, erasure, restriction of processing, communication of a personal data breach to the data subject or confidentiality of communication.

Article 2

Specification of the controller and safeguards

1. The safeguards in place to avoid data breaches, leakages or unauthorised disclosure are the following:

- (a) Paper documents shall be kept in secured cupboards and only accessible to authorized staff;
- (b) All electronic data shall be stored in a secure IT application according to the ENISA’s security standards, as well as in specific electronic folders accessible only to authorised staff. Appropriate levels of access shall be granted individually;
- (c) The database shall be password-protected under a single sign-on system and connected automatically to the user’s ID and password. Replacing users is strictly prohibited. E-records shall be held securely to safeguard the confidentiality and privacy of the data therein;
- (d) All persons having access to the data are bound by the obligation of confidentiality.

2. The controller of the processing operations is ENISA, represented by its Executive Director, who may delegate the function of the controller. Data subjects shall be informed of the delegated controller by way of the data protection notices or records published on the website and/or the intranet of ENISA.

3. The retention period of the personal data referred to in Article 1(3) shall be no longer than necessary and appropriate for the purposes for which the data are processed. It shall in any event not be longer than the retention period specified in the data protection notices, privacy statements or records referred to in Article 5(1).

4. Where ENISA considers to apply a restriction, the risk to the rights and freedoms of the data subject shall be weighed, in particular, against the risk to the rights and freedoms of other data subjects and the risk of cancelling the effect of the ENISA's investigations or procedures for example by destroying evidence. The risks to the rights and freedoms of the data subject concern primarily, but are not limited to, reputational risks and risks to the right of defence and the right to be heard.

Article 3

Restrictions

1. Any restriction shall only be applied by ENISA to safeguard:

(a) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(b) other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

(c) the internal security of Union institutions and bodies, including of their electronic communications networks;

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) and (b);

(f) the protection of the data subject or the rights and freedoms of others.

2. The assessment of cybersecurity incidents carried out by ENISA pursuant to Article 7(4) of the Regulation (EU) 2019/881 (Cybersecurity Act) falls under paragraph 1 point (b) of this Article.

3. As a specific application of the purposes described in paragraph 1 above, ENISA may apply restrictions in relation to personal data exchanged with Commission services or other Union institutions, bodies, agencies and offices, competent

authorities of Member States or third countries or international organisations, respectively in the following circumstances:

(a) where the exercise of those rights and obligations could be restricted by Commission services or other Union institutions, bodies, agencies and offices on the basis of other acts provided for in Article 25 of Regulation (EU) 2018/1725 or in accordance with Chapter IX of that Regulation or with the founding acts of other Union institutions, bodies, agencies and offices;

(b) where the exercise of those rights and obligations could be restricted by competent authorities of Member States on the basis of acts referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council, or under national measures transposing Articles 13(3), 15(3) or 16(3) of Directive (EU) 2016/680 of the European Parliament and of the Council;

(c) where the exercise of those rights and obligations could jeopardise ENISA's cooperation with third countries or international organisations in the conduct of its tasks.

Before applying restrictions in the circumstances referred to in points (a) and (b) of the first subparagraph, ENISA shall consult the relevant Commission services, Union institutions, bodies, agencies, offices or the competent authorities of Member States unless it is clear to ENISA that the application of a restriction is provided for by one of the acts referred to in those points.

4. Any restriction shall be necessary and proportionate taking into account the risks to the rights and freedoms of data subjects and respect the essence of the fundamental rights and freedoms in a democratic society.

5. If the application of restriction is considered, a necessity and proportionality test shall be carried out based on the present rules. It shall be documented through an internal assessment note for accountability purposes on a case by case basis.

6. Restrictions shall be lifted as soon as the circumstances that justify them no longer apply. In particular, where it is considered that the exercise of the restricted right would no longer cancel the effect of the restriction imposed or adversely affect the rights or freedoms of other data subjects.

Article 4

Review by the Data Protection Officer

1. ENISA shall, without undue delay, inform the Data Protection Officer of the Agency ('the DPO') whenever the controller restricts the application of data subjects' rights, or extends the restriction, in accordance with this Decision. The controller shall provide the DPO access to the record containing the assessment of the necessity and proportionality of the restriction and document the date of informing the DPO in the record. ENISA shall involve the DPO throughout all the relevant procedures and the DPO's involvement shall be documented.

2. The DPO may request the controller in writing to review the application of the restrictions. The controller shall inform the DPO in writing about the outcome of the requested review.

3. The controller shall inform the DPO when the restriction has been lifted.

Article 5

Provision of information to data subject

1. In duly justified cases and under the conditions stipulated in this Decision, the right to information may be restricted by the controller in the context of the following processing operations:

- a) the performance of administrative inquiries and disciplinary proceedings;
- b) preliminary activities related to cases of potential irregularities reported to OLAF;
- c) whistleblowing procedures;
- d) (formal and informal) procedures for cases of harassment;
- e) processing internal and external complaints;
- f) internal audits;
- g) the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation 2018/1725;
- h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU);
- i) assessments of cybersecurity incidents carried out by ENISA pursuant to Article 7(4) of the Regulation (EU) 2019/881, in line with Article 3 paragraph 2 of this Decision.

ENISA shall include in the data protection notices, privacy statements or records in the sense of Article 31 of the Regulation (EU) 2018/1725, published on its website and/or on the intranet informing data subjects of their rights in the framework of a given procedure, information relating to the potential restriction of these rights. The information shall cover which rights may be restricted, the reasons and the potential duration.

2. Without prejudice to the provisions of paragraph 3 of this Article, ENISA, where proportionate, shall also inform individually all data subjects, which are considered persons concerned in the specific processing operation, of their rights concerning present or future restrictions without undue delay and in a written form.

3. Where ENISA restricts, wholly or partly, the provision of information to the data subjects referred to in paragraph 2 of this Article, it shall record the reasons for the restriction, the legal ground in accordance with Article 3 of this Decision, including an assessment of the necessity and proportionality of the restriction.

The record and, where applicable, the documents containing underlying factual and legal elements shall be registered. Upon request, they shall be made available to the European Data Protection Supervisor.

4. The restriction referred to in paragraph 3 of this Article shall continue to apply as long as the reasons justifying it remain applicable.

Where the reasons for the restriction no longer apply, ENISA shall provide information to the data subject on the principal reasons on which the application of a restriction is based. At the same time, ENISA shall inform the data subject of the right of lodging a complaint with the European Data Protection Supervisor at any time or of seeking a judicial remedy in the Court of Justice of the European Union.

ENISA shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry, procedure or investigation. Thereafter, the controller shall monitor the need to maintain any restriction every six months.

Article 6

Right of access by data subject

1. In duly justified cases and under the conditions stipulated in this Decision, the right to access may be restricted by the controller in the context of the following processing operations, where necessary and proportionate:

- a) the performance of administrative inquiries and disciplinary proceedings;
- b) preliminary activities related to cases of potential irregularities reported to OLAF;
- c) whistleblowing procedures;
- d) (formal and informal) procedures for cases of harassment;
- e) processing internal and external complaints;
- f) internal audits;
- g) the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation 2018/1725;
- h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU);
- i) assessments of cybersecurity incidents carried out by ENISA pursuant to Article 7(4) of the Regulation (EU) 2019/881, in line with Article 3 paragraph 2 of this Decision.

Where data subjects request access to their personal data processed in the context of one or more specific cases or to a particular processing operation, in

accordance with Article 17 of Regulation (EU) 2018/1725, ENISA shall limit its assessment of the request to such personal data only.

2. Where ENISA restricts, wholly or partly, the right of access, referred to in Article 17 of Regulation (EU) 2018/1725, it shall take the following steps:

(a) it shall inform the data subject concerned, in its reply to the request, of the restriction applied and of the principal reasons thereof, and of the possibility of lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy in the Court of Justice of the European Union;

(b) it shall document in an internal assessment note the reasons for the restriction, including an assessment of the necessity, proportionality of the restriction and its duration.

The provision of information referred to in point (a) may be deferred, omitted or denied if it would cancel the effect of the restriction in accordance with Article 25(8) of Regulation (EU) 2018/1725.

ENISA shall review the application of the restriction every six months from its adoption and at the closure of the relevant investigation. Thereafter, the controller shall monitor the need to maintain any restriction every six months.

3. The record and, where applicable, the documents containing underlying factual and legal elements shall be registered. They shall be made available to the European Data Protection Supervisor on request.

Article 7

Right of rectification, erasure and restriction of processing

1. In duly justified cases and under the conditions stipulated in this Decision, the right to rectification, erasure and restriction may be restricted by the controller in the context of the following processing operations, where necessary and appropriate:

- a) the performance of administrative inquiries and disciplinary proceedings;
- b) preliminary activities related to cases of potential irregularities reported to OLAF;
- c) whistleblowing procedures;
- d) (formal and informal) procedures for cases of harassment;
- e) processing internal and external complaints;
- f) internal audits;
- g) the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation 2018/1725;

- h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU);
- i) assessments of cybersecurity incidents carried out by ENISA pursuant to article 7(4) of the Regulation (EU) 2019/881, in line with Article 3 paragraph 2 of this Decision.

2. Where ENISA restricts, wholly or partly, the application of the right to rectification, erasure and restriction of processing referred to in Articles 18, 19(1) and 20(1) of Regulation (EU) 2018/1725, it shall take the steps set out in Article 6(2) of this Decision and in accordance with Article 6(3) thereof.

Article 8

Communication of a personal data breach to the data subject and confidentiality of electronic communications

1. In duly justified cases and under the conditions stipulated in this Decision, the right to the communication of a personal data breach may be restricted by the controller in the context of the following processing operations, where necessary and appropriate:

- a) the performance of administrative inquiries and disciplinary proceedings;
- b) preliminary activities related to cases of potential irregularities reported to OLAF;
- c) whistleblowing procedures;
- d) processing internal and external complaints;
- e) internal audits;
- f) the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation 2018/1725;
- g) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU);
- e) assessments of cybersecurity incidents carried out by ENISA pursuant to article 7(4) of the Regulation (EU) 2019/881, in line with Article 3 paragraph 2 of this Decision.

2. In duly justified cases and under the conditions stipulated in this Decision, the right to confidentiality of electronic communications may be restricted by the controller in the context of the following processing operations, where necessary and appropriate:

- a) the performance of administrative inquiries and disciplinary proceedings;

- b) preliminary activities related to cases of potential irregularities reported to OLAF;
- c) whistleblowing procedures;
- d) formal procedures for cases of harassment;
- e) processing internal and external complaints;
- f) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).
- g) assessments of cybersecurity incidents carried out by ENISA pursuant to Article 7(4) of the Regulation (EU) 2019/881, in line with Article 3 paragraph 2.

3. Where ENISA restricts the communication of a personal data breach to the data subject or the confidentiality of electronic communications referred to in Articles 35 and 36 of Regulation (EU) 2018/1725, it shall apply the provisions of Article 5(3) of this Decision. Article 5(4) of this Decision shall apply.

Article 9

Entry into force

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

Done at Athens, on 21 November 2019

For ENISA

[signed]

Chairperson of the Management Board

Jean Baptiste Demaison