DECISION

EFSA – European Food Safety Authority	**Decision 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 EFSA**	**No.: mb190619-a6**
	Effective Date: *(Day following publication in the EU Official Journal)*	**Supersedes**: NA

Approvals	Signature	Name
Originator		Bernhard Url
Management Board	See Decision	Jaana Husu-Kallio (Chair of the Management Board)

Introduction	On 11 December 2018, Regulation (EU) 2018/1725 entered into force, aligning the rules on data protection and privacy in EU institutions, bodies and agencies (EUIs) with those applicable in the European Union based on the General Data Protection Regulation (GDPR) (EU) 2016/679 that became applicable few months earlier. The new data protection Regulation for EUIs *inter alia* details the rights of data subjects, including the right of information, the right of access and rectification, the right to erasure ('right to be forgotten'). In certain circumstances the legally warranted rights may be restricted based on internal rules adopted by the EUI in accordance with Article 25 of the Regulation. Indent (5) of Article 25 requires that the internal rules shall be adopted at the highest level of management and be subject to publication in the Official Journal of the EU. Likewise, EFSA Internal Rules to restrict data subjects' rights are proposed for adoption by the Management Board prior to their publication in the EU Official Journal. The present Decision is based on a template developed in a Working Group of Data Protection Officers (DPOs) of EUIs on which the European Data Protection Supervisor (EDPS) was consulted.
Description	EFSA is bound to respect, to the maximum extent possible, the fundamental rights of data subjects, in particular, the right for information, access and rectification, the right to erasure, restriction of processing, the right of communication of a personal data breach to the data subject and the confidentiality of electronic communications laid down in Regulation (EU) No 2018/1725. However, in certain situations, EFSA may be obliged to restrict these data subject's rights to protect, in particular, its own investigations or procedures, those of other public authorities, and/or the rights of other persons concerned by the investigations or proceedings in question. The present Decision details the specific conditions and modalities for restricting on a case-by-case basis specific data subject's rights warranted in Regulation (EU) No 2018/1725.
References	Regulation (EU) 2018/1725, especially Article 25
Abbreviations	*See Decision*

DECISION OF THE EUROPEAN FOOD SAFETY AUTHORITY

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 EFSA

THE MANAGEMENT BOARD

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 European Parliament and Council Regulation (EC) No 178/2002 of 28 January 2002 establishing the European Food Safety Authority ('EFSA') and laying down procedures in relation to food safety[2], and in particular Articles 25, 26 and 48,

Having regard to the rules of procedure of EFSA's Management Board[3] and in particular Article 8 thereof,

Having regard to the Opinion of the European Data Protection Supervisor ('the EDPS') of 14 May 2019 and to the EDPS Guidance on Article 25 of the new Regulation and internal rules,

After consulting the Staff Committee,

Whereas:

1) EFSA carries out its activities in accordance with its Founding Regulation (EC) No 178/2002.

2) 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 EFSA, where these are not based on legal acts adopted on the basis of the Treaties.

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

([1]) OJ L 295, 21.11.2018, p. 39

[2] OJ L 31, 1.2.2002, p.1, as last amended.

[3] mb 27 06 13 – Revised Management Board Rules of Procedure – ADOPTED.

4) Where EFSA 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) Within the framework of its administrative functioning, EFSA 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, carry out investigations by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and internal (IT) security investigations.

   EFSA 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).

6) EFSA, represented by its Executive Director, acts as the overall data controller irrespective of further delegations of the controller role within EFSA to reflect operational responsibilities for specific personal data processing.

7) 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 EFSA.

8) The internal rules should apply to all processing operations carried out by EFSA 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, 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).

9) 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 EFSA to national authorities and international organisations outside of its administrative investigations.

10) In the cases where these internal rules apply, EFSA 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.

11) Within this framework EFSA 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.

12) However, EFSA may be obliged to restrict the information to the 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.

13) EFSA may thus restrict the information for the purpose of protecting the investigation and the fundamental rights and freedoms of other data subjects.

14) EFSA should periodically monitor that the conditions that justify the restriction apply and lift the restriction as far as they do no longer apply.

15) The Controller should inform the Data Protection Officer at the moment of deferral and during the revisions.

HAS ADOPTED THIS DECISION:

Article 1
Subject matter and scope

1. This Decision lays down rules relating to the conditions under which EFSA in the framework of its procedures set out in 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 EFSA, this Decision applies to the processing operations on personal data by EFSA 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, 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 EFSA 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 electronic communications.

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 EFSA's security standards, as well as in specific electronic folders accessible only to authorised staff. Appropriate levels of access shall be granted individually;
(c) Databases shall be password-protected under EFSA's single sign-on system, associated automatically with the user's ID and password and supported by a secure information access management system. Electronic records shall be held securely ensuring confidentiality and compliance with data protection rules and principles;
(d) All persons having access to the data are bound by the obligation of confidentiality.

2. The controller of the processing operations is EFSA, 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 EFSA's website, intranet portal, and/or the Business Services Catalogue.

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 EFSA 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 EFSA'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 EFSA 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. As a specific application of the purposes described in paragraph 1 above, EFSA 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, 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 EFSA'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) above , EFSA shall consult the relevant Commission services, Union institutions, bodies, agencies, offices or the competent authorities of Member States unless it is clear to EFSA that the application of a restriction is provided for by one of the acts referred to in those points.

3. 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.

4. If the application of a 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.

5. 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. In such case, the restrictions will be lifted as soon as possible and as a rule within five working days from the alteration in the legal or factual circumstances.

Article 4
Review by the Data Protection Officer

1. EFSA shall, without undue delay, inform the Data Protection Officer of EFSA (´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.

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 (EU) 2018/1725;

(h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

EFSA shall include in the data protection notices, privacy statements or records in the sense of Article 31 of 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, EFSA, 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 EFSA restricts, wholly or partly, the provision of information to the data subjects referred to in paragraph 2, 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. They shall be made available to the European Data Protection Supervisor on request.

4. The restriction referred to in paragraph 3 shall continue to apply as long as the reasons justifying it remain applicable and shall be lifted as soon as possible and as a rule within five working days from the alteration in the legal or factual circumstances.

Where the reasons for the restriction no longer apply, EFSA shall provide information to the data subject on the principal reasons on which the application of a restriction is based. At the same time, EFSA 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.

EFSA shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry, procedure or investigation.

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 (EU) 2018/1725;

(h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

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, EFSA shall limit its assessment of the request to such personal data only.

2. Where EFSA 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.

EFSA shall review the application of the restriction every six months from its adoption and at the closure of the relevant investigation.

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 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 (EU) 2018/1725;

(h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

2. Where EFSA 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 register the record 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 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 (EU) 2018/1725;

(h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

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 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 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).

3. Where EFSA 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 record and register the reasons for the restriction in accordance with 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.

Adopted in Parma on 19 June 2019

For EFSA's Management Board

[NOT SIGNED]

Jaana Husu-Kallio

Chair of the Management Board