RULES OF PROCEDURE

DECISION OF THE STEERING COMMITTEE OF THE EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES

on internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the Agency

THE STEERING COMMITTEE,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249(1) thereof,

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]) ('the Regulation'), and in particular Article 25 thereof,

Having regard to Commission Implementing Decision 2013/771/EU of 17 December 2013 establishing the 'Executive Agency for Small and Medium-sized Enterprises' and repealing Decisions 2004/20/EC and 2007/372/EC ([2]),

Having consulted the European Data Protection Supervisor,

Whereas:

(1) The Executive Agency for Small and Medium-sized Enterprises (EASME) ('the Agency') was established by Implementing Decision 2013/771/EU in view of the performance of tasks linked to the implementation of Union programmes in the field of energy, environment, climate action, competitiveness and SMEs, research and innovation and ICT ([3]).

(2) Within the framework of its administrative and operational functioning, the Agency may conduct administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings in accordance with the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ('Staff Regulations') ([4]) and with implementing provisions regarding the conduct of administrative inquiries and disciplinary proceedings. If required the Agency may carry out preliminary activities related to cases of potential fraud and irregularities and may notify cases to OLAF.

(3) Agency staff members are under an obligation to report potentially illegal activities, including fraud and corruption, which are detrimental to the interests of the Union. Staff members are also obliged to report conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the obligations of officials of the Union. This is regulated by the internal rules or policies concerning whistleblowing.

([1]) OJ L 295, 21.11. 2018, p. 39.

([2]) Commission Implementing Decision 2013/771/EU of 17 December 2013 establishing the 'Executive Agency for Small and Medium-sized Enterprises' and repealing Decisions 2004/20/EC and 2007/372/EC (OJ L 341, 18.12.2013, p. 73), and the EASME financial statement, as amended by EASME financial statement on 2 October 2014.

([3]) Commission Decision C(2013) 9414 of 23 December 2013 delegating powers to the Executive Agency for Small and Medium-sized Enterprises with a view to performance of tasks linked to the implementation of Union programmes in the field of energy, environment, climate action, competitiveness and SMEs, research and innovation and ICT, comprising, in particular, implementation of appropriations entered in the general budget of the Union, as last amended by Commission Decision C(2019) 3353 of 30 April 2019 and its Annex.

([4]) Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

(4) The Agency has put in place a policy to prevent and deal effectively with actual or potential cases of psychological or sexual harassment in the workplace, as provided for in implementing measures pursuant to the Staff Regulations establishing an informal procedure whereby the alleged victim of the harassment can contact the Agency's 'confidential' counsellors.

(5) The Agency can also conduct internal (IT) security investigations and on potential breaches of security rules for European Union classified information ('EUCI').

(6) The Agency is subject to both internal and external audits concerning its activities, including conducted by the Internal Audit Services of the European Commission and the European Court of Auditors.

(7) The Agency may handle requests from the European Public Prosecutors office (EPPO), requests for access to medical files of Agency staff members, carry out investigations by the Data Protection Officer in line with Article 45(2) of the Regulation.

(8) In the context of such administrative inquiries, audits, investigations or requests, the Agency cooperates with other Union institutions, bodies, offices and agencies.

(9) The Agency may cooperate with third countries' national authorities and international organisations, either at their request or on its own initiative.

(10) The Agency may also cooperate with EU Member States' public authorities, either at their request or on its own initiative.

(11) The Agency may be subject to complaints, proceeding or investigations via whistle-blowers or the European Ombudsman.

(12) The Agency may be involved in cases before the Court of Justice of the European Union when it either refers a matter to the Court, defends a decision it has taken and which has been challenged before the Court, or intervenes in cases relevant to its tasks. In this context, the Agency may need to preserve the confidentiality of personal data contained in documents obtained by the parties or the interveners.

(13) In the context of its activities the Agency processes several categories of personal data, including identification data of natural persons, contact information, professional roles and tasks, information on private and professional conduct and performance, and financial data as well as in some specific cases sensitive data (e.g. health data). Personal data includes factual 'hard' data and 'soft' assessment data.

'Hard data' is objective factual data such as identification data, contact data, professional data, administrative details, metadata related to electronic communications and traffic data.

'Soft data' is subjective data and include in particular the description and assessment of situations and circumstances, opinions, observations related to data subjects, evaluation of the conduct and performance of data subjects and reasoning underpinning individual decisions related to or brought forward in connection with the subject matter of the procedure or activity carried out by the Agency in line with the applicable legal framework.

Assessments, observations and opinions are considered personal data in the meaning of Article 3(1) of the Regulation.

(14) Under the Regulation, the Agency is therefore obliged to provide information to data subjects on those processing activities and to respect their rights as data subjects.

(15) The Agency is committed to respect, to the maximum extent possible, the fundamental rights of the data subjects in particular, the right of provision of information, access and rectification, the right to erasure, restriction of processing, the right of communication of a personal data breach to the data subject or confidentiality of communication as enshrined in the Regulation. However, the Agency may also be required to restrict data subject's rights and obligations for the purpose of protecting its activities and the fundamental rights and freedoms of others.

(16) Therefore Article 25(1) and (5) of the Regulation, gives the Agency the possibility to restrict, under conditions, the application of Articles 14 to 22, 35 and 36, as well as Article 4 of the Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 20 shall be based on internal rules to be adopted at the highest level of management of the Agency and subject to publication in the Official Journal of the European Union, where they are not based on legal acts adopted on the basis of the Treaties.

(17) Restrictions may apply to different data subject rights, including the 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 as enshrined in the Regulation.

(18) The Agency may be required to reconcile those rights with the objectives of administrative inquiries, audits, investigations and court proceedings. It may also be required to balance a data subject's rights against the fundamental rights and freedoms of other data subjects.

(19) The Agency may, for instance, need to restrict the information it provides to a data subject about the processing of his or her personal data during the preliminary assessment phase of an administrative inquiry or during the inquiry itself, prior to a possible dismissal of case or at the pre-disciplinary stage. In certain circumstances, providing such information may seriously affect the Agency's capacity to conduct the inquiry in an effective way, whenever, for example, there is a risk that the person concerned may destroy evidence or interfere with potential witnesses before they are interviewed. The Agency may also need to protect the rights and freedoms of witnesses as well as those of other persons involved.

(20) The Agency may need to protect the anonymity of a witness or whistle-blower who has asked not to be identified. In such a case, the Agency may decide to restrict access to the identity, statements and other personal data of such persons or the suspect, in order to protect their rights and freedoms.

(21) The Agency may need to protect confidential information concerning a staff member who has contacted Agency's confidential counsellors in the context of a harassment procedure. In such cases, the Agency may need to restrict access to the identity, statements and other personal data of the alleged victim, the alleged harasser and other persons involved, in order to protect the rights and freedoms of all concerned individuals.

(22) In relation to selection and recruitment procedures, staff evaluation and public procurement procedures the right to access, rectification, erasure and restriction can be exercised only at certain points in time and under the conditions as provided for in the relevant procedures in order to safeguard the rights of other data subjects and to respect the principles of equal treatment and the secrecy of deliberations.

(23) The Agency may also restrict access of individuals to their medical data for instance of psychological or psychiatric nature due to the potential sensitivity of these data, and the medical service of the Commission may want to give the data subjects only indirect access through their own practitioner. The data subject may exercise the right to rectification of assessments or opinions of the Commission's Medical service by providing their comments or a report of a medical practitioner of their choice.

(24) The Agency, represented by its Director, acts as the data controller irrespective of further delegations of the controller role within the Agency to reflect operational responsibilities for specific personal data processing activities to competent 'delegated data controllers'.

(25) The personal data are stored securely in an electronic environment compliant with Commission Decision (EU, Euratom) 2017/46 ([5]) 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 and records of the Agency.

([5]) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

(26) The Agency shall apply restrictions only when they respect the essence of fundamental rights and freedoms, are strictly necessary and are a proportionate measure in a democratic society. The Agency shall give reasons explaining the justification for those restrictions and inform accordingly the data subjects on those grounds and their right to lodge a complaint to the EDPS as provided for by Article 25(6) of the Regulation.

(27) In application of the principle of accountability, the Agency shall keep a record of its application of restrictions.

(28) When processing personal data exchanged with other organisations in the context of its tasks, the Agency and those organisations shall consult each other on potential grounds for imposing restrictions and the necessity and proportionality of those restrictions, unless this would jeopardise the activities of the Agency.

(29) These internal rules shall thus apply to all processing activities carried out by the Agency involving personal data in the performance of administrative inquiries, disciplinary proceedings, preliminary activities related to cases of potential irregularities reported to OLAF, investigations of the European Public Prosecutors office (EPPO), whistleblowing procedures, (formal and informal) procedures for cases of harassment, processing of internal and external complaints, requests of access to or rectification of own medical files, the investigations carried out by the Data Protection Officer in line with Article 45(2) of the Regulation, (IT) security investigations handled internally or with external involvement (e.g. CERT-EU), audits, proceedings before the Court of Justice of the European Union or national public authorities, selection and recruitment procedures, staff evaluation and public procurement, as listed above.

(30) These internal rules shall apply to processing activities carried out prior to the launch 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 the Agency to other EU Institutions, national authorities and international organisations outside of its administrative investigations.

(31) Pursuant to Article 25(8) of the Regulation, the Agency is entitled to defer, omit or deny the provision of information on the reasons for the application of a restriction to the data subject if this would in any way cancel the effect of the restriction. The Agency shall assess on a case-by-case basis whether the communication of the restriction would cancel its effect.

(32) The Agency shall lift the restriction as soon as the conditions that justify the restriction no longer apply, and assess those conditions on a regular basis.

(33) To guarantee utmost protection of the rights and freedoms of data subjects and in accordance with Article 44(1) of the Regulation, the Data Protection Officer of the Agency shall be consulted in due time before any restriction may be applied or reviewed and verify its compliance with this Decision.

(34) Articles 16(5) and 17(4) of the Regulation provide for exceptions to data subjects' right to information and right of access. If these exceptions apply, the Agency does not need to apply a restriction under this Decision,

HAS ADOPTED THIS DECISION:

Article 1

Subject matter and scope

1. This Decision lays down rules relating to the conditions under which the Executive Agency for Small and Medium-sized Enterprises (EASME) and any of its legal successor ('the Agency') may restrict the application of Articles 4, 14 to 22, 35 and 36, pursuant to Article 25 of the Regulation.

2. The Agency, as the Data controller, is represented by the Director of the Agency, who may delegate further the function of the Data controller.

Article 2

Applicable restrictions

1. The Agency may restrict the application of Articles 14 to 22, 35 and 36, as well as Article 4 of the Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 20.

2. This Decision applies to the processing of personal data by the Agency within the framework of its administrative and operational functioning:

(a) pursuant to Article 25(1)(b), (c), (f), (g) and (h) of the Regulation when conducting internal investigations, including based on external complaints, administrative inquiries, pre-disciplinary, disciplinary or suspension proceedings under Article 86 and Annex IX of the Staff Regulations and its implementing rules, security investigations or OLAF investigations;

(b) pursuant to Article 25(1)(h) of the Regulation, when ensuring that Agency's staff members may report facts confidentially where they believe there are serious irregularities, as set out in the internal rules or policies concerning whistleblowing;

(c) pursuant to Article 25(1)(h) of the Regulation, when ensuring that Agency's staff members are able to report to confidential counsellors in the context of a harassment procedure, as defined by internal rules;

(d) pursuant to Article 25(1)(c), (g) and (h) of the Regulation, when conducting internal or external audits in relation to activities or the functioning of the Agency;

(e) pursuant to Article 25(1)(d) and (h) of the Regulation, when ensuring security analyses, including cyber security and IT system abuses, handled internally or with external involvement (e.g. CERT-EU), ensuring internal security by means of video surveillance, access control and investigation purposes, securing communication and information systems and carrying out technical security counter measures;

(f) pursuant to Article 25(1)(g) and (h) of the Regulation, when the Data Protection Officer ('DPO') of the Agency investigates matters directly related to the his/her tasks;

(g) pursuant to Article 25(1)(b), (g) and (h) of the Regulation, in the context of investigations from the European Public Prosecutor Office (EPPO);

(h) pursuant to Article 25(1)(h) of the Regulation, when individuals request to access or rectify their medical data, including if they are held by the Commission's Medical Service.

(i) pursuant to Article 25(1)(c), (d), (g) and (h) of the Regulation, when providing or receiving assistance to or from other Union institutions, bodies, offices and agencies or cooperating with them in the context of activities under points (a) to (h) of this paragraph and pursuant to relevant service level agreements, memoranda of understanding and cooperation agreements of their respective establishment act;

(j) pursuant to Article 25(1)(c), (g) and (h) of the Regulation, when providing or receiving assistance to or from third countries national authorities and international organisations or cooperating with such authorities and organisations, either at their request or on its own initiative;

(k) pursuant to Article 25(1)(c), (g) and (h) of the Regulation, when providing or receiving assistance and cooperation to and from EU Member States' public authorities, either at their request or on its own initiative;

(l) pursuant to Article 25(1)(e) of the Regulation, when processing personal data in documents obtained by the parties or interveners in the context of proceedings before the Court of Justice of the European Union.

For the purpose of this Decision, the above activities shall include preparatory and follow-up actions directly related to the same activity.

3. The Agency may also apply restrictions on a case-by-case basis to data subjects' rights referred to in this Decision, in the following circumstances:

(a) where the Commission services or other Union institutions, bodies, agencies and offices are entitled to restrict the exercise of the listed rights and the purpose of such a restriction by that Commission Service, Union institution, body or agency would be jeopardised where the Agency does not apply an equivalent restriction in respect of the same personal data;

(b) where the competent authorities of Member States are entitled to restrict the exercise of the listed rights and the purpose of such a restriction by that Member State authority would be jeopardised where the Agency does not apply an equivalent restriction in respect of the same personal data;

(c) where the exercise of those rights and obligations would jeopardise the Agency's cooperation with third countries or international organisations in the conduct of its tasks, unless this need to cooperate is overridden by the interests or fundamental rights and freedoms of the data subject;

(d) before applying restrictions under this paragraph, the Agency shall consult where necessary the relevant Commission services, other Union institutions, bodies, agencies, offices, international organisations or the competent authorities of Member States, unless it is clear that the restriction is provided for by one of the acts referred to above or such a consultation would jeopardise the Agency's activities.

4. The categories of personal data processed related to the above activities may contain factual 'hard' data and 'soft' assessment data.

5. Any restriction shall respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.

Article 3

Recording and registering of restrictions

1. The Data controller shall draw up a record of the restriction describing:

(a) the reasons for any restriction applied pursuant to this Decision;

(b) which grounds among those listed in Article 2 apply;

(c) how the exercise of the right would present a risk for the data subject or would jeopardise the purpose of the Agency's tasks or would adversely affect the rights and freedoms of other data subjects;

(d) outcome of the assessment of the necessity and proportionality of the restriction, taking into account the relevant elements in Article 25(2) of the Regulation.

2. A necessity and proportionality test of a restriction shall be carried out on a case-by-case basis before restrictions are applied. The Data controller shall consider the potential risks to the rights and freedoms of the data subject. Restrictions shall be limited to what is strictly necessary to achieve their objective.

3. The record of the restriction 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 4

Risks to the rights and freedoms of data subjects

1. Assessments of the risks to the rights and freedoms of data subjects of imposing restrictions and details of the period of application of those restrictions shall be registered in the record of processing activities maintained by the data controller based on Article 31 of the Regulation. They shall also be recorded in any data protection impact assessments regarding those restrictions conducted under Article 39 of the Regulation, when applicable.

2. Where the data controller considers applying 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 negatively impacting 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 5

Safeguards and storage periods

1. The Agency shall put in place specific safeguards to prevent abuse and unlawful access or transfer of personal data in respect of which restrictions apply or could be applied. Such safeguards shall include technical and organisational measures and be detailed as necessary in the Agency's internal decisions, procedures and implementing rules. These safeguards shall include:

(a) a clear definition of roles, responsibilities and procedural steps;

(b) if appropriate, a secure electronic environment which prevents unlawful and accidental access or transfer of electronic data to unauthorised persons;

(c) if appropriate, secure storage and processing of paper-based documents;

(d) ensure compliance with confidentiality obligations for all persons having access to the personal data.

2. The retention period of personal data under a restriction shall be defined in the related record under Article 31 of the Regulation taking into account the purpose of the processing and shall include the timeframe necessary for administrative and judicial review. At the end of the retention period, the personal data shall be deleted, anonymised or transferred to archives in accordance with Article 13 of the Regulation.

Article 6

Duration of restrictions

1. Restrictions referred to in Article 2 shall continue to apply as long as the reasons justifying them remain applicable.

2. Where the reasons for a restriction no longer apply, the Data controller shall lift the restriction if the exercise of the restricted right would no longer negatively impact the relevant applicable procedure or adversely affect the rights or freedoms of other data subjects.

3. In case the data subject has asked again for access to the personal data concerned, the Data controller shall provide the principal reasons for the restriction to the data subject. At the same time, the Agency shall inform the data subject of the possibility 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.

4. The Agency shall review the application of the restrictions referred to in Article 2 every six months.

Article 7

Involvement of the Data Protection Officer

1. The data controller of the Agency shall inform the DPO of the Agency without undue delay and prior to any decision to restrict data subject rights in accordance with this Decision or to extend the application of the restriction. The data controller shall provide the DPO access to the associated records and any document concerning the factual or legal context.

2. The DPO may request the data controller to review the application of a restriction. The data controller shall inform the DPO in writing of the outcome of the requested review.

3. The data controller shall document the involvement of the DPO in the application of the restriction, including what information is shared. The documents under this article shall be part of the record related to the restriction and made available to the EDPS on request.

Article 8

Information to data subject on restrictions of their rights

1. The data controller shall include in the data protection notices and records under Article 31 of the Regulation, published on its website and on the Intranet general information on the potential restrictions of data subjects' rights pursuant to Article 2(2) of this decision. The information shall cover which rights and obligations may be restricted, the grounds on which restrictions may be applied and their potential duration.

2. The data controller shall inform data subjects individually, in writing and without undue delay of ongoing or future restrictions of their rights. The data controller shall inform the data subject of the principal reasons on which the application of the restriction is based, of their right to consult the DPO with a view to challenging the restriction and of their rights to lodge a complaint with the EDPS.

3. The data controller may defer, omit or deny the provision of information concerning the reasons for a restriction and the right to lodge a complaint with the EDPS for as long as it would cancel the effect of the restriction. The assessment of this justification shall take place on a case-by-case basis and the data controller shall provide the information to the data subject, as soon as this would no longer cancel the effect of the restriction.

Article 9

Right of access by data subject

1. In duly justified cases and under the conditions stipulated in this Decision, the right to access under Article 17 of the Regulation may be restricted by the data controller where necessary and proportionate with regards to the activities under this Decision.

2. Where data subjects request access to their personal data processed in the context of a specific processing activity referred to in Article 2(2) of this Decision, the Agency shall limit its response to the personal data processed for that activity.

3. The data subjects rights to directly access the documents of a psychological or psychiatric nature may be restricted. Neither indirect access, nor the right to rectification and communication of a personal data breach shall be limited with these internal rules. Therefore, an intermediary physician should be granted access on request of the concerned individual to all related information and discretionary power as to how and what access to provide to the data subject.

4. Where the data controller restricts, wholly or partly, the right of access to personal data, as referred to in Article 17 of the Regulation, it shall inform the data subject concerned in writing, in its reply to the request for access, of the restriction applied and of the principal reasons thereof and of the possibility of lodging a complaint with the EDPS or of seeking a judicial remedy in the Court of Justice of the European Union.

5. The information on the restriction of access may be deferred, omitted or denied if it would cancel the effect of the restriction in accordance with Article 25(8) of the Regulation.

6. A restriction under this article shall be applied in accordance with this Decision.

Article 10

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 of processing under Articles 18, 19(1) and 20(1) of the Regulation may be restricted by the data controller where necessary and appropriate, with regards to activities under Article 2(2) of this Decision.

2. In relation to medical data, data subjects may exercise the right to rectification of the assessment or opinion of the Commission's Medical Service by providing their comments or a report of a medical practitioner of their choice including, directly to the Commission's Medical Service.

3. A restriction under this article shall be applied in accordance with this Decision.

Article 11

Communication of a personal data breach to the data subject

1. Where the data controller is under an obligation to communicate a data breach under Article 35(1) of the Regulation, he/she may, in exceptional circumstances, restrict such communication wholly or partly. He/she shall document in a note the reasons for the restriction, the legal ground for it under Article 2 and an assessment of its necessity and proportionality. The note shall be communicated to the EDPS at the time of the notification of the personal data breach.

2. Where the reasons for the restriction no longer apply, the Agency shall communicate the personal data breach to the data subject concerned and inform him or her of the principal reasons for the restriction and of his or her right to lodge a complaint with the EDPS.

Article 12

Confidentiality of electronic communications

1. In exceptional circumstances, the Agency may restrict the right to confidentiality of electronic communications provided for by Article 36 of the Regulation. Such restrictions shall comply with Directive 2002/58/EC of the European Parliament and of the Council.

2. Notwithstanding Article 8(3), where the Agency restricts the right to confidentiality of electronic communications, it shall inform the data subject concerned, in its reply to any request from the data subject, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the EDPS.

Article 13

Entry into force

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

Done at Brussels, 9 November 2020.

For the EASME Steering Committee
(e-signed)
Kristin SCHREIBER
The Chairperson