RULES OF PROCEDURE

DECISION OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

of 26 March 2020

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 the European Union Intellectual Property Office

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]), and in particular Article 25 thereof,

Having regard to Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark ([2]), and in particular Article 153 thereof,

Having regard to the Rules of Procedure of the Management Board of the European Union Intellectual Property Office, and in particular Article 9 thereof,

Having regard to the consultation of the European Data Protection Supervisor on 18 December 2019,

Whereas:

(1) The European Union Intellectual Property Office (the 'Office') carries out its activities in accordance with Regulation (EU) 2017/1001.

(2) In line 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 insofar 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 the Office, where these are not based on legal acts adopted on the basis of the Treaties.

(3) These internal rules, including their provisions on the assessment of the necessity and proportionality of a restriction, do not apply where a legal act adopted on the basis of the Treaties provides for a restriction of the rights of data subjects.

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

(5) Under its administrative functioning, the Office may be obliged to restrict the rights of data subjects following Article 25 of Regulation (EU) 2018/1725.

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

(7) The personal data is 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 is retained as specified in the data protection notices, privacy statements or records of the Office.

([1]) OJ L 295, 21.11.2018, p. 39.
([2]) OJ L 154, 16.6.2017, p. 1.

(8) These internal rules should apply to all processing operations carried out by the Office in the context of administrative inquiries, disciplinary proceedings, whistleblowing procedures, (formal and informal) procedures for dealing with harassment, processing complaints and medical data, conducting internal audits, investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and Information Technology (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

(9) In cases where these internal rules apply the Office has to explain why the restrictions are strictly necessary and proportionate in a democratic society and respect the essence of fundamental rights and freedoms.

(10) Within this framework the Office is bound to respect, to the maximum extent possible, the fundamental rights of the data subjects during the above procedures, in particular, those on the right to information, access and rectification, right to erasure, restriction of processing, right of communication of a personal data breach to the data subjects or confidentiality of communication as enshrined in Regulation (EU) 2018/1725.

(11) The Office should periodically monitor that the conditions that justify the restriction apply and lift the restriction as far as it does no longer apply.

(12) The Controller should inform the Data Protection Officer of each restriction applied to the data subject's rights, when the restriction has been lifted or when the restriction has been revised.

HAS ADOPTED THIS DECISION:

Article 1

Subject matter and scope

1. This Decision lays down rules on the conditions under which the Office in the framework of its processing operations set out in paragraph 2 may restrict the application of the rights enshrined in Articles 4, 14 to 21, 35 and 36 of Regulation (EU) 2018/1725, following Article 25 thereof.

2. Under the administrative functioning of the Office, this Decision applies to the processing of personal data by the Office for the purposes of: administrative inquiries, disciplinary proceedings, whistleblowing procedures, (formal and informal) procedures for dealing with harassment, processing complaints, processing medical data and/or files, 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).

This Decision applies to processing operations initiated and carried out by the Office, including 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 also applies to assistance and cooperation provided by the Office, outside its own administrative procedures, to OLAF, competent authorities of Member States and/or other competent authorities.

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 the Office performs its duties with respect to the rights of data subjects 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 subjects or confidentiality of electronic communications.

Article 2

Specification of the controller and safeguards

1. The Office shall put in place the following safeguards to prevent abuse or unlawful access or transfer:

(a) paper documents shall be kept in secured cupboards and only accessible to authorised staff;

(b) all electronic data shall be stored in a secure IT application according to the Office's security standards, as well as in specific electronic folders accessible only to authorised staff. Appropriate levels of access shall be granted individually;

(c) IT systems and their databases must have mechanisms for verifying user's identity under a single sign-in system and connected automatically to the user's ID and password. End-user accounts must be unique, personal and non-transferrable, sharing user accounts 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 the Office, 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 Office's intranet.

3. The retention period of the personal data referred to in Article 1(3) shall be no longer than specified in the data protection notices, privacy statements or records referred to in Article 3(1). At the end of the retention period, the case related information, including personal data, is deleted, anonymised or transferred to the historical archives.

4. Where the Office 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 hindering the purpose of the processing operation. 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. The Office shall publish on its website and/or on the intranet data protection notices, privacy statements and/or records in the sense of Article 31 of Regulation (EU) 2018/1725, informing all data subjects of its activities involving processing of their personal data and of their rights in the framework of a given procedure, including information on a potential restriction of these rights. The information shall cover which rights may be restricted, the reasons and the potential duration.

2. Subject to the provisions of paragraph 3, where relevant, the Office shall ensure that the data subjects are informed individually in an appropriate format. The Office may also individually inform them about their rights concerning present or future restrictions.

3. Any restriction initiated by the Office shall only be applied to safeguard the purposes enumerated under Article 25(1) of Regulation (EU) 2018/1725:

(a) the national security, public security or defence of the Member States;

(b) 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;

(c) 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;

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

(e) the protection of judicial independence and judicial proceedings;

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

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

(h) the protection of the data subject or the rights and freedoms of others;

(i) the enforcement of civil law claims.

4. In particular, when the Office restricts in the context of:

(a) administrative inquiries and disciplinary proceedings, restrictions may be based on Article 25(1)(c), (e), (g), (h) of Regulation (EU) 2018/1725;

(b) whistleblowing procedures, restrictions may be based on Article 25(1)(h) of Regulation (EU) 2018/1725;

(c) (formal and informal) procedures for dealing with harassment, restrictions may be based on Article 25(1)(h) of Regulation (EU) 2018/1725;

(d) processing complaints, restrictions may be based on Article 25(1)(c), (e), (g), (h) of Regulation (EU) 2018/1725;

(e) processing medical data, restrictions may be based on Article 25(1) (h) of Regulation (EU) 2018/1725;

(f) internal audits, restrictions may be based on Article 25(1)(c), (g), (h) of Regulation (EU) 2018/1725;

(g) investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725, restrictions may be based on Article 25(1)(c), (g), (h) of Regulation (EU) 2018/1725;

(h) IT security investigations handled internally or with external involvement (e.g. CERT-EU), restrictions may be based on Article 25(1)(c), (d), (g), (h) of Regulation (EU) 2018/1725.

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

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. The test will also be conducted in the context of reviewing the application of a restriction.

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.

6. In addition, the Office may be requested to exchange personal data of data subjects with Commission services or other EU institutions, bodies, agencies and offices, competent authorities of Member States or other competent authorities from third countries or international organisations, including:

(a) where the Commission services or other EU institutions, bodies, agencies and offices restrict their obligations and the exercise of the rights of these data subjects 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 EU institutions, bodies, agencies and offices;

(b) where the competent authorities of Member States restrict their obligations and the exercise of the rights of these data subjects on the basis of acts referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([3]), 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 ([4]).

Wherever the exchange of personal data is initiated by another authority, no restriction is applied by the Office and the case related information, including personal data, shall be deleted or anonymised by the Office upon transmission of the requested data to that authority.

7. The records on the restrictions and, where applicable, the documents containing underlying factual and legal aspects shall be made available to the European Data Protection Supervisor on request.

Article 4

Review by the Data Protection Officer

1. The Office shall, without undue delay, inform the Data Protection Officer of the Office ('the DPO') whenever the controller restricts the application of the rights of data subjects, lifts the restriction or revises the period of 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 the DPO is informed 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 involvement of the DPO in the restrictions procedure, including information exchanges, shall be documented in an appropriate form.

Article 5

Provision of information to data subject

1. In duly justified cases and under the conditions stipulated in this Decision, the provision of information may be restricted by the controller, where necessary and proportionate, in the context of the processing operations provided for in Article 1(2) of this Decision. In particular, the provision of information may be deferred, omitted or denied if it would cancel the effect of the processing operation.

2. Where the Office restricts, wholly or partly, the provision of information referred to in paragraph 1, 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.

3. The restriction referred to in paragraph 1 shall continue to apply as long as the reasons justifying it remain applicable.

Where the reasons for the restriction no longer apply, the Office shall provide information to the data subject on the principal reasons for the restriction. At the same time, the Office shall inform the data subject 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.

4. The Office shall review the application of the restriction at least once a year and at the closure of the relevant procedure. Thereafter, the controller shall monitor the need to maintain any restriction on an annual basis.

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([4]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

Article 6

Right of access, rectification, erasure and restriction of processing by data subject

1. In duly justified cases and under the conditions stipulated in this Decision, the right to access, rectification, erasure and restriction of processing may be restricted by the controller, where necessary and proportionate, in the context of the processing operations provided for in Article 1(2) of this Decision. The provisions contained in this present Article 6 do not apply to the right of access to medical data and/or files, for which specific rules are explicitly provided for under Article 7 below.

2. Where data subjects request to exercise their right of access, rectification, erasure and restriction of processing concerning their personal data processed in the context of one or more specific cases or concerning a particular processing operation, the Office shall limit its assessment of the request to such personal data only.

3. Where the Office restricts, wholly or partly, the right of access, rectification, erasure and restriction of processing, 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.

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

4. The Office shall review the application of the restriction of the rights of the data subjects at least once a year and at the closure of the relevant procedure. Thereafter, upon request of data subjects, the controller shall review the need to maintain the restriction.

Article 7

Right of access to medical data and/or files

1. Restriction of the right of access of data subjects to their medical data and/or files requires specific provisions which are stipulated under this article.

2. Subject to the below paragraphs of this article, the Office may restrict data subject's right to access directly personal medical data and/or files of a psychological or psychiatric nature concerning them which are processed by the Office, where access to such data is likely to represent a risk for the data subject's health. This restriction shall be proportionate to what is strictly necessary to protect the data subject.

3. Access to the information referred to in paragraph 2 shall be given to a doctor of the data subject's choice.

4. In such cases, the data subject shall, upon request, be reimbursed by the Medical Service of the part of the cost of the medical consultation with the doctor who received access to the medical data and/or files that has not been reimbursed by the Joint Sickness Insurance Scheme (JSIS). The reimbursement shall not exceed the difference between the ceiling laid down in the General Implementing Provisions for the reimbursement of medical expenses ([5]) and the amount reimbursed to the data subject by the JSIS according to those rules.

5. Such reimbursement by the Medical Service shall be subject to the condition that access has not already been granted for the same data and/or files.

6. Subject to the below paragraphs of this article, the Office may restrict, on a case by case basis data subject's right to access their personal medical data and/or files in its possession, in particular where the exercise of that right would adversely affect the rights and freedoms of the data subject or other data subjects.

([5]) Commission Decision C(2007) 3195 of 2 July 2007 laying down General Implementing Provisions for the reimbursement of medical expenses.

7. Where data subjects request to exercise their right of access to their personal data processed in the context of one or more specific cases or to a particular processing operation, the Office shall limit its assessment of the request to such personal data only.

8. Where the Office restricts, wholly or partly, the right of access to personal medical data and/or files by data subjects, 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, notably by stating how the exercise of the right would present a risk for the data subject's health or would adversely affect the rights and freedoms of the data subjects or other data subjects.

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

9. Restrictions referred to in the above paragraphs 2 and 6 shall continue to apply as long as the reasons justifying them remain applicable. Once the reasons for a restriction no longer apply, upon request of data subjects, the controller shall review the need to maintain the restriction.

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, where necessary and appropriate in the context of the processing operations provided for in Article 1(2) of this Decision. This right shall however not be restricted in the context of the procedures for dealing with harassment.

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, where necessary and appropriate in the context of the processing operations provided for in Article 1(2) of this Decision.

3. Article 5(2), (3) and (4) of the present Decision applies where the Office 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.

Article 9

Entry into force

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

Done at Alicante, 26 March 2020.

For the European Union Intellectual Property Office
Jorma HANSKI
Chairperson of the Management Board