

EUROPEAN DATA PROTECTION SUPERVISOR

# Guidance on Article 25 of the new Regulation and internal rules



December 2018

## **Executive Summary**

Data protection is a fundamental right, which contains ‘rights within the right’ such as the right of information, access, rectification, portability, right to erasure etc. These rights should be scrupulously respected but according to EU secondary legislation they could be restricted in some exceptional circumstances and with the safeguards laid down in the new Regulation. The Union institutions and bodies should adopt such restrictions only where strictly necessary and always based on a legal act or, in absence of such legal act, on internal rules adopted by the highest level of management and published on the Official Journal of the European Union.

Restrictions done on the basis of internal rules are only possible in matters relating to the operation of the Union institutions and bodies. Consultation of the EDPS when drawing up internal rules is required.

On the basis of the internal rules and for accountability purposes, the controller should draft a ‘proportionality and necessity test assessment note’ which analyses the need for the restriction. This note should specify which rights are being restricted as well as the reasons and the duration of the restriction. The Data Protection Officer should be consulted all along the process.

The present guidance paper focuses on the conditions under which internal rules may restrict these rights, how to draw up them and how to interpret and apply restrictions in a concrete case.

## List of recommendations:

### 1) On internal rules

- R1:** Perform a necessity and proportionality test on the need for restriction in your organisation;
- R2:** Only draw up internal rules to restrict data subject rights with a clear legal basis;
- R3:** Allow for restrictions to the least extent possible (a ‘restriction within the restriction’ should apply as regards to the rights and the extent of the restriction);
- R4:** Internal rules should provide for temporary restrictions, to be lifted when their causes no longer apply;
- R5:** Consult the Data Protection Officer (hereinafter ‘DPO’) when drawing up the internal rules;
- R6:** Consult the European Data Protection Supervisor when drawing up the internal rules;
- R7:** Review your internal rules when necessary.

### 2) On the application of a restriction in a concrete case

- R1:** Perform a necessity and proportionality test on the need for restriction;
- R2:** Ensure that there is a general data protection notice that informs data subjects including on potential restrictions;
- R3:** Restrict on a case-by-case basis only;
- R4:** Restrict to the least extent possible (a ‘restriction within the restriction’ should apply as regards to the rights and the extent of the restriction);
- R5:** Restrictions should be temporary and be lifted when their causes no longer apply;
- R6:** Consult the DPO before and during the restriction<sup>1</sup>;
- R7:** Document restrictions for accountability purposes;
- R8:** Monitor your restriction on a regular basis.

---

<sup>1</sup> The controller should involve the DPO all along the procedure and document this consultation.

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>4</b>
<b>2. WHAT IS A RESTRICTION?.....</b>	<b>5</b>
<b>3. WHICH RIGHTS MAY BE AFFECTED BY A RESTRICTION? .....</b>	<b>6</b>
<b>4. WHAT ARE THE CONDITIONS FOR ANY RESTRICTION? .....</b>	<b>8</b>
4.1 Necessity and proportionality test .....	8
4.2 Need for a legal basis. ....	9
4.3 Grounds for restricting .....	9
4.3.1 <i>The national security, public security or defence of the Member States.</i> .....	9
4.3.2 <i>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.</i> .....	10
4.3.3 <i>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.</i> .....	11
4.3.4 <i>The internal security of Union institutions and bodies, including of their electronic communication networks.</i> .....	11
4.3.5 <i>The protection of judicial independence and judicial proceedings</i> .....	12
4.3.6 <i>The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions</i> .....	12
4.3.7 <i>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) of paragraph 1 of Article 25 of the new Regulation</i> .....	12
4.3.8 <i>The protection of the data subject or the rights and freedoms of others</i> .....	13
4.3.9 <i>The enforcement of civil law claims</i> .....	13
<b>5. HOW TO DRAFT INTERNAL RULES AND IMPLEMENT THEM.....</b>	<b>13</b>
5.1 The principles .....	13
5.2 Hands on: the internal rules .....	14
<b>6. INFORMATION ABOUT RESTRICTIONS .....</b>	<b>15</b>
6.1 General information .....	15
6.2 Specific cases .....	16
<b>7. CONCLUSION .....</b>	<b>16</b>
<b>ANNEX I: ARTICLE 25 OF THE REGULATION.....</b>	<b>18</b>
<b>ANNEX II: MODEL OF INTERNAL RULES.....</b>	<b>20</b>
<b>ANNEX III: INTERNAL NOTE ON A CONCRETE RESTRICTION- NECESSITY AND PROPORTIONALITY TEST MODEL.....</b>	<b>25</b>
<b>ANNEX IV: MODEL – EXTRACT OF GENERAL DATA PROTECTION NOTICE INFORMING ON THE POSSIBLE RESTRICTIONS.....</b>	<b>27</b>

## 1. Introduction

1. Fundamental rights and freedoms are at the core of the EU democracies. The EDPS has the duty to ensure that the work of the European Union institutions, agencies, offices and bodies (hereinafter ‘EUIs’) is guided by the most scrupulous respect for the protection of fundamental rights and freedoms of individuals in relation to the processing of personal data. The protection of personal data should be designed to serve humankind<sup>2</sup> and, within this context, one of the main objectives of data protection law is to enhance data subjects’ control over their data.
2. In order to guarantee this control, data subjects have a number of rights *within* the right to data protection. Data protection cannot be conceived without the rights it guarantees. The right of access and the right to rectification are enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter ‘Charter’). The new Regulation (EU) 2018/1725 (hereinafter “Regulation”)<sup>3</sup> contains those rights and complements them with a number of additional rights, some already existed to a large extent in Regulation 45/2001<sup>4</sup> such as the right to object and erasure<sup>5</sup>, and others are new such as portability rights.
3. The importance of the rights of access, to rectification, erasure etc. cannot be underestimated. They are at the core of the fundamental right to data protection and their application should be the general rule. It is against this background that Article 25 of the new Regulation should be read and interpreted. This provision is headed ‘restrictions’ and it states that in a number of situations duly enumerated, the EUIs may restrict the application of certain provisions of the Regulation, mainly relating to the rights of the data subjects. **This is the exception to the general rule and, as such, should remain of limited application. As every exception to the general rule, the controller should be able to demonstrate its application**<sup>6</sup>.
4. According to Article 52(1) of the Charter<sup>7</sup>, any limitation on the exercise of the rights and freedoms recognised by the Charter must be ‘provided for by law’. This corresponds to

---

<sup>2</sup> Recital 4 of 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1.

<sup>3</sup> 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, (Text with EEA relevance), OJ L 295, 21.11.2018, p. 39.

<sup>4</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.

<sup>5</sup> Now this right is also called ‘right to be forgotten’.

<sup>6</sup> A restriction is different from an exception such as those gathered in Article 16(5).

<sup>7</sup> Article 52(1) of the Charter provides that ‘any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality,

the expression ‘in accordance with the law’ in Article 8(2) of the European Convention of Human Rights (hereinafter ‘ECtHR’), which means not only compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. In particular, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures<sup>8</sup>. The same strict standard should be required for any restrictions that could be imposed by EUIs. Consequently, in its Opinion 5/2017 on the Proposal for the new Regulation, the EDPS considered that, ‘in order to ensure compliance with the quality of law requirements referred to above, [...] only legal acts adopted on the basis of the Treaties should be able to restrict fundamental rights, thus imposing on EU institutions the same standards that would apply to Member States under the GDPR’. The new Regulation provides nonetheless that, in matters relating to the operation of EUIs, restrictions may be provided for by internal rules. Therefore, **restrictions should mainly be provided for by legal acts and it is only in these matters and in absence of such legal act, where necessity is rightly proved, that restrictions may be provided for by internal rules.**

5. **This guidance paper explains when the EUIs may apply the restrictions and how to draft internal rules that constitute the legal basis for such restrictions<sup>9</sup>.** On the basis of the previous Regulation, restrictions could be done on a case-by-case basis provided that they were justified. With the new legislation, restrictions have to be backed by a secondary Union legal act or, in matters relating to the operation of a EUI, by fully-fledged internal rules adopted at the highest level of the EUI. **Therefore, this is a new development from the old regulation.**

## 2. What is a restriction?

6. The Oxford dictionary defines a restriction as a ‘limiting condition or measure, specially a legal one’<sup>10</sup>. Data subject rights can be restricted but not denied. Restriction is *per se* a temporary measure (for instance, as long as the investigation takes places) but when the circumstances that justified the restriction no longer apply, the rights of the data subjects have to be ‘returned’. For example it may be appropriate not to inform suspects in an early stage of an investigation not to jeopardise that investigation. Nevertheless, when these persons are being interrogated they should receive information about their rights.
7. A restriction must always respect the essence of the right that is being restricted. This means that limitations that are so extensive and intrusive to devoid a fundamental right of its basic content cannot be justified. If the essence of the right is compromised, the

---

limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.’

<sup>8</sup> *Malone v United Kingdom*, [1984] ECHR 10, paragraph 67; *Leander v Sweden*, [1987] 9 EHRR 433, paragraphs. 50-51; *Halford v United Kingdom*, [1997] ECHR 32, paragraph 49.

<sup>9</sup> The specific derogations that may be provided for where personal data are processed for scientific or historical research purposes, statistical purposes and archiving purposes in the public interest will be addressed in a separate paper (Articles 25 (3) and (4) of the new Regulation).

<sup>10</sup> <https://en.oxforddictionaries.com/definition/restriction>

limitation must be considered unlawful, without the need to further assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria<sup>11</sup>.

8. The EDPS Necessity Toolkit has provided that one has to examine whether the essence of the right is respected, that is, '[...] whether the right is in effect emptied of its basic content and the individual cannot exercise the right. If the essence of the right is affected, the measure is unlawful and there is no need to proceed further with the assessment of its compatibility with the rules set in Article 52(1) of the Charter<sup>12</sup>.

### 3. Which rights may be affected by a restriction?

9. The data subjects' rights and EUIs' obligations that may be restricted under Article 25(1) are exclusively those provided by **Articles 14 to 22 of the Regulation** as well as **Articles 35 and 36** of the Regulation.
10. Firstly, the right of information to the data subject may be restricted. **Article 14** is about transparent information to the data subjects, including communication and modalities for the exercising of their rights. **Articles 15 and 16** concern the information to be given to the data subject in two different case scenarios (when data were collected from the data subjects and when data were not collected from them respectively)<sup>13</sup>. This restriction should not apply to general data protection notices which include information about the possibility to restrict information during a period of time (for a model see Annex III). This is to ensure compliance with the principle of fairness. The Working Party 29 (hereinafter 'WP 29') has stated that '[a]s such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on so that the data subject is not taken by surprise at a purported restriction of a particular right when the later attempts to exercise it against the controller<sup>14</sup>.
11. Secondly, the application of **Articles 17 and 18** can be restricted. These provisions cover the rights of access and to rectification of the data subjects. For instance, the right of access to a decision opening an administrative inquiry can be restricted temporarily not to hamper the preliminary steps of the inquiry. This is also the case when for an opening decision of the European Anti-Fraud Office (hereinafter 'OLAF') investigation or for the transmission

---

<sup>11</sup> See point 1.2.2 of the Handbook of European data protection law, 2018 edition, Publications Office of the European Union (pages 44 and 45). To illustrate this, the following case law is quoted: CJEU judgment of 6 October 2015, C-362/14 Maximilian Schrems v Data Protection Commissioner and CJEU judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources and Others and Karntner Landesregierung and Others.

<sup>12</sup> EDPS Necessity Toolkit, page 4 at: [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_en\\_0.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf).

<sup>13</sup> Concerning transparency and information to data subjects, see the 'Guidance paper Articles 14-16 of the new regulation 45/2011 transparency rights and obligations': [https://edps.europa.eu/sites/edp/files/publication/18-01-15\\_guidance\\_paper\\_arts\\_en\\_1.pdf](https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf)

<sup>14</sup> Paragraph 68 of the WP 29 'Guidelines on transparency under Regulation 2016/679', adopted on 29 November 2017, last revised and adopted on 11 April 2018 and endorsed on 25 May 2018 by the European Data Protection Board (page 33).

of a case to OLAF. Right to rectification may be restricted, for instance, during the time of this type of investigations.

12. Thirdly, the application of **Article 19** on right to erasure (also called ‘right to be forgotten’) can be restricted. This right applies often when there is an issue about the lawfulness of data processing operation or when the data are no longer relevant and the data subject has requested their deletion. Restricting the right to erasure means that the data subject will not be able to have data deleted that, under normal circumstances, would have been suppressed.
13. Fourthly, **Article 20** is about the right to restriction of processing and **Article 21** about the need to notification regarding any restriction carried out in accordance with Article 20 as well as any rectification and erasure. The right to restriction is the former right to have data blocked.
14. Finally, **Article 22** concerns the right to data portability. This is a new right and may concern transfers of (electronic) files.
15. It is important to note that the right to object cannot be restricted under Article 25 (1)<sup>15</sup>. The data subject always has a right to object to processing of personal data where such processing is based on the necessity ‘for the performance of a task carried out in the public interest or in the exercise of official authority’. In practice, under the circumstances described above, the data subject always has a right to complain. However, the controller has to examine the objection and may demonstrate that there are compelling legitimate grounds not to accept it<sup>16</sup>.
16. Finally, **Articles 35 and 36 of the Regulation** can also be restricted: these provisions concern the communication of a data breach to the data subject and the confidentiality of electronic communications<sup>17</sup>. Given that a restriction to the confidentiality of electronic communications may interfere with the essence of the right to privacy, it is only under extraordinary circumstances that this right can be restricted<sup>18</sup>.

---

<sup>15</sup> This right allows data subjects to object to lawful processing on grounds relating to their particular situation.

<sup>16</sup> Article 23 (1) states as follows: ‘the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (a) of Article 5(1), including profiling based on that provision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.’

<sup>17</sup> See the Guidelines on personal data and electronic communications in the EU institutions, February 2015 at: [https://edps.europa.eu/sites/edp/files/publication/15-12-16\\_ecommunications\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/15-12-16_ecommunications_en.pdf)

<sup>18</sup> Accordingly, any restriction of this right would have to correspond to the high standards laid down in the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37 (or the forthcoming ePrivacy Regulation [see Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final]). See also EDPS Guidelines on Data Breaches published on 11 December 2018.



17. In addition, a limitation may concern **Article 4 of the Regulation**. This provision covers the principles relating to the processing of personal data (lawfulness, transparency, purpose limitation or data minimisation etc.). Any restriction of the application of Article 4, such as transparency, must relate to the restriction of rights and obligations stated in Articles 14 to 22. For instance, if the right of access is being restricted in the framework of an investigation, the transparency principle as stated in Article 4 is as a consequence affected.

## 4. What are the conditions for any restriction?

### 4.1 Necessity and proportionality test

18. To be lawful, any limitation on the exercise of the fundamental rights protected by the Charter must comply with the following criteria, laid down in Article 52(1) of the Charter:
- it must be provided for by law,
  - it must respect the essence of the rights,
  - it must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others,
  - it must be necessary and
  - it must be proportional.
19. This list of criteria sets out the required order of the assessment of lawfulness. First it must be examined whether an accessible and foreseeable law provides for a limitation, and whether the essence of the right is respected<sup>19</sup>. The following test is whether the measure meets an objective of general interest. The objective of general interest provides the background against which the necessity of the measure may be assessed. It is therefore important to identify the objective of general interest in sufficient detail so as to allow the assessment as to whether the measure is necessary<sup>20</sup>. The next step is to **assess the necessity of the envisaged restrictions**. The case law of the Court of Justice of the European Union applies a *strict necessity* test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data: *'derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary'*. The ECtHR applies a test of *strict necessity* depending on the context and all circumstances at hand, such as with regard to secret surveillance measures<sup>21</sup>.
20. If this test is satisfied, the **proportionality of the envisaged measure** will be assessed. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure which is not proved to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity<sup>22</sup>.

---

<sup>19</sup> See para 8 of this guidance paper.

<sup>20</sup> See in this regard section 4.3. of this guidance paper on the grounds for restricting.

<sup>21</sup> For more guidance on how to apply the necessity test, please refer to the EDPS Necessity Toolkit available at: EDPS Necessity Toolkit, page 4 at: [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_en\\_0.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf)

<sup>22</sup> For further guidance on how to apply the proportionality test, please refer to the forthcoming EDPS Proportionality Toolkit.

21. The necessity and proportionality test will typically imply **assessing the risks to the rights and freedoms of the data subjects. The overall assessment should be mentioned in the internal rules.**

#### 4.2 Need for a legal basis.

22. Pursuant to the new Regulation, any restriction has to be either based on a legal act adopted on the basis of the Treaties or, in absence of such a legal basis, in matters relating to the operation of EUIs, on internal rules of the EUIs. It is no longer possible to impose *ad hoc* restrictions for specific cases. This is a difference from the previous Regulation<sup>23</sup>, where restrictions were based on Article 20 exclusively.
23. The EUIs should thus ensure that there is a clear legal basis before applying any restriction and, when this basis is found in internal rules, they must ensure their publication in Official Journal of the European Union. The present paper will focus on restrictions that are based on internal rules.

#### 4.3 Grounds for restricting

24. In order to adopt internal rules for restrictions and to apply a restriction, one or several of the following conditions have to be met. This list is exhaustive which means that restrictions cannot be done under other conditions than those enumerated below.
25. Based on the internal rules as published, the controller should draft an **internal confidential note** that analyses which rights are going to be restricted, the reasons and the timing. This note is necessary for accountability purposes. The controller should thus perform a *necessity and proportionality test* on the restriction that it intends to apply. In other words, the controller should document why it is necessary to restrict as well as how it intends to comply with the requirement of non-restricting more than necessary<sup>24</sup>.
26. The controller should revise that note when necessary (Annex II); the DPO should always be informed and, if possible, involved in the assessment.

##### 4.3.1 The national security, public security or defence of the Member States.

27. A restriction to data subject's rights can have as a basis, national or public security and/ or defence of the Member States. Concerning restrictions based on national security, this has often been associated with surveillance and processing of data for intelligence purposes<sup>25</sup>.

---

<sup>23</sup> On the basis of Article 20 of Regulation 45/2001, the EUIs could apply directly a restriction based on that Regulation without the need for internal rules or any other specific legal basis.

<sup>24</sup> See WP 29 Opinion on some key issues of the Law Enforcement Directive, adopted on 29 November 2017. Although limited to the law enforcement context point 4 on limitations to the right of access, in its last paragraph stated that '[...] where the right of access is restricted or refused, Member States must provide that controllers document the factual or legal reasons for such decision and such information must be made available to the supervisory authorities upon request.' For further guidance see also the Necessity Toolkit as quoted in footnote 10

<sup>25</sup> See point 2 of the WP 29 Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) adopted on 13 April 2016. The Working Document states: 'this right of countries to introduce legislation intended to maintain national security or to collect data for intelligence

28. Moreover, public security includes protection of human life especially in response to natural or manmade disasters. In addition, one cannot exclude that the EUIs may need to apply this restriction in exceptional cases such as terrorist attacks or national disasters, should there be a sound basis for this.

#### **4.3.2 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.**

29. Regulation 45/2001 already foresaw the first part of the indent, this is, the ‘prevention, investigation, detection and prosecution of criminal offences’<sup>26</sup>. The new Regulation adds the second part; this is the ‘execution of criminal penalties’ and ‘including the safeguarding against and the prevention of threats to public security’.

30. Even if the wording refers to investigation of *criminal offences*, this has to be interpreted broadly as covering administrative inquiries, disciplinary proceedings or OLAF investigations as far as there is a connection with the prevention, investigation of criminal offences. This restriction may apply to OLAF in the course of their investigations but also to EUIs that notify potential cases of irregularities to OLAF and request an investigation. The same applies for EUIs that notify cases to Commission’s Investigation and Disciplinary Office (‘IDOC’) for investigations, provided that this relates to criminal offences. In summary, when EUIs refer cases to OLAF or IDOC, during a certain period of time, rights can be restricted<sup>27</sup>.

31. The EDPS has recognised that ‘providing information to the data subject while the investigation is still ongoing could jeopardise the success of the said investigation...’<sup>28</sup> The omitted information must, in accordance with the case law of the Court of Justice of the EU, be provided once it is no longer liable to jeopardise the investigation being carried out<sup>29</sup>. This means that as soon as it is possible a specific (tailor-made) data protection

---

purposes is naturally also recognised by the WP 29. Moreover, intelligence gathering can be a perfectly legitimate aim to process personal data, as has also been underlined by the ECtHR, most recently in the Szabó case.’

<sup>26</sup> By the same token, Article 36 (6) (c) of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53, provides that access rights of data subjects may be restricted to ‘guarantee that any national investigation will not be jeopardised’.

<sup>27</sup> In the Guidelines on the rights of individuals with regard to processing of personal data issued under Regulation 45/2001, referred to in footnote 11, the EDPS recognised that this notion ‘also covers disciplinary proceedings and administrative inquiries. It therefore applies, for example, to investigations carried out by the European Anti-fraud Office (OLAF) and the Commission’s Investigations and Disciplinary Office (IDOC).’ See pages 27 and 28.

<sup>28</sup> See Guidelines mentioned above, page 28.

<sup>29</sup> Opinion 1/15 of the Court of Justice of the European Union (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017.

notice must be given to the data subject stating the different rights such as access, rectification etc.

In cases involving **OLAF investigations**, the EDPS has pointed out in relation to the equivalent provision under Regulation 45/2001, that ‘...even if one of the exemptions under Article 20(1) applies, Article 20(3) obliges the controller to inform the data subject of the principal reasons for deferring access and the right to seek recourse to the EDPS. Article 20(4) establishes that in these cases, when investigating complaints by data subjects, the EDPS shall only inform the data subject whether data have been processed correctly and if not, whether the necessary corrections have been made. According to Article 20(5), this information may be deferred as long as it would deprive the restriction imposed under Article 20(1) of its effect.’<sup>30</sup>

32. It should be pointed out that, before restricting rights in the framework of an administrative proceeding, investigation or similar, the EUI should ensure that the formal procedure has been opened. In particular, if there are connexions with criminal offences it is by all means safer for the EUI to restrict rights within the framework of a formal investigation than outside this framework. As a matter of principle, EUIs should ensure that they post a fully-fledged data protection notice in their websites informing potential data subjects on the potential temporary restriction of their rights (see Annex III). The EUIs should also draft specific data protection notices once access and other rights are no longer liable to jeopardise the investigation being carried out.

**4.3.3 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.**

33. The EDPS had used this exception in the past in the field of procurement and grant procedures for the right to rectification of personal data insofar as this right could only be exercised up to the closing date for submission of application of tenders. Other examples may concern investigations carried out by some services of the Commission such as DG Trade or DG COMP provided that they serve important objectives of public interest of the Union.

**4.3.4 The internal security of Union institutions and bodies, including of their electronic communication networks.**

34. Ensuring internal security may involve video surveillance for security purposes, control of access to and within EUI buildings or securing communication and information systems of EUIs. The rights that could be restricted on the ground of internal security of EUIs would mainly be the right to information and confidentiality of electronic communications. The EUIs should define in advance the restrictions of data subject rights and the conditions under which it can be done.

---

<sup>30</sup> See joint cases 2010-0797, 2010-0798 and 2010-0799.

#### **4.3.5 The protection of judicial independence and judicial proceedings**

35. Any restriction of this kind could be applied by the Court of Justice of the EU in the exercise of their judicial function.

#### **4.3.6 The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions**

36. This could be the case of certain administrative inquires or disciplinary proceedings that are opened *vis-à-vis* the data subject for breaches of the Staff or Financial Regulations, such as disclosure of information covered by confidentiality rules, some cases of harassment, conflict of interests etc.<sup>31</sup> Those are cases in which an investigation is carried out by the institution, IDOC (or eventually by OLAF) but there is no connection in principle with criminal offences as, in that case, point 4.2.3 would be applicable. This being said the borderline between the present cases and those stated in point 4.1.3 may not always be clear-cut, so in case of doubt both legal bases could be used for a given restriction.
37. As it is the case for the prevention and investigation of criminal offences referred to above, it is important that the EUI first opens an administrative procedure, which can be an inquiry or an investigation as it is much safer to restrict rights within this framework in case of dispute or litigation.

In the case of harassment, the EDPS has noted that exceptions under Article 20 (of Regulation 45/2001) would most probably be used to defer the right of access of the alleged harasser to his/her own data<sup>32</sup>. The reason is of course the protection of the alleged victim. The right of access of the alleged harasser depends on the information that he or she has; he or she will not request access if he or she is not aware of an existing informal procedure involving him or her. The application of the limitations must be dealt with on a case-by-case basis by the controller balancing the rights of the alleged harasser with the protection of the potential victim.

#### **4.3.7 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) of paragraph 1 of Article 25 of the new Regulation**

38. This restriction refers to a potential limitation when there is an inspection or a monitoring exercise or a regulatory function connected, even occasionally to the exercise of official authority in the cases referred to in points 4.3.1 to 4.3.2. included, performed by a EUI. It could be the case of a targeted audit for instance or an inspection in the framework of an investigation. In these cases, nevertheless a general data protection notice should be given to the data subject or posted in the internet/intranet of the EUI. As an example, during the

---

<sup>31</sup> For more examples please see: [https://ec.europa.eu/info/about-european-commission/service-standards-and-principles/codes-conduct/ethics-and-integrity-eu-commissioners/rules-commissioners-regarding-ethics-and-integrity\\_e](https://ec.europa.eu/info/about-european-commission/service-standards-and-principles/codes-conduct/ethics-and-integrity-eu-commissioners/rules-commissioners-regarding-ethics-and-integrity_e)

<sup>32</sup> See case 2011-0483 (non published).

time of audit of a recruitment procedure of a given staff member, their right to rectification can be partially restricted.

#### 4.3.8 The protection of the data subject or the rights and freedoms of others

39. The EDPS used this ground in the past for restrictions in cases of alleged harassment in order to protect the alleged victim or during an investigation to protect witnesses or whistle-blowers in cases where personal data relate to the suspect as well (allegations made about the suspect by informants or witnesses).
40. Furthermore this exception could also be used in the framework of the medical services of a given institution, in order to restrict access to medical data of psychological or psychiatric nature. Given the potential sensitivity of some of these data the medical service of a given institution may want to give the data subject indirect access through his or her own practitioner.

#### 4.3.9 The enforcement of civil law claims

Even if this kind of restriction seems to apply more at the national level; in any case it is a new ground to apply a restriction which did not appear in the previous regulation.<sup>33</sup>

## 5. How to draft internal rules and implement them

### 5.1 The principles

41. Internal rules should be **clear and precise and of general application**. A model is provided in this Guidance document (Annex IV) but the internal rules can be tailor-made to the specific needs of each processing operation as well as to the specific needs of each EUI. Before drafting internal rules it is advisable that the EUI makes a global exercise of identification of which (categories of) processing operations need to be covered by the internal rules. A necessity test on the need to apply restrictions, at the general level of the EUI should also be performed<sup>34</sup>.
42. A set of internal rules can **cover one or several processing operations**. For instance, there may be internal rules for restrictions within the scope of administrative inquiries only but there could be also internal rules that cover several processing operations such as administrative inquiries, disciplinary proceedings and transmission of cases to OLAF and/or IDOC. For simplification purposes, an EUI could issue one set of internal rules that may cover several situations.
43. The rules have to be intended to **produce legal effects vis-a-vis data subjects** and adopted at **the highest level of management** of the EUIs. Once adopted they have to be **published in the Official Journal of the European Union** as well as in the intranet and internet website of the institution.

---

<sup>33</sup> This rule comes from the GDPR and it seems to fit more within a national context.

<sup>34</sup> For further information on how to conduct such necessity test, see the EDPS Necessity Toolkit, footnote 10.

44. On the basis of Article 41 (2) of the new Regulation, the EDPS should be consulted when the EUI is drawing up the internal rules<sup>35</sup>.
45. On the basis of these rules, each time that an EUI needs to impose a restriction it should first do a ‘necessity and proportionality test’ that will be duly documented (see Annex II). This assessment could be either made on its own or, for simplification reasons, be attached to the decision opening the inquiry, investigation etc. This document should be reviewed periodically to examine whether the conditions that justified the restriction still apply.
46. As a matter of good practice, the DPO should be involved in the drafting of the internal rules, the ‘proportionality and necessity test assessment note’ and in the subsequent reviews.

## 5.2 Hands on: the internal rules

47. The Regulation requires that EUIs draft internal rules governing the restrictions. The rules shall -in principle- or where relevant, as the regulation states, contain specific provisions on a number of issues that will be described here below.
48. The internal rules should, first of all, refer to the **purpose of the processing or categories of processing**, for instance the need to open administrative inquiries or disciplinary proceedings, notification of cases to OLAF, the need to conduct investigations, etc.
49. The rules should refer to **the categories of personal data**. This means that the categories of data should be specified, whether restriction of access concerns data relating to administrative proceedings, data of administrative nature, medical data etc. The restriction thus concerns the categories of data but the controller may go one-step beyond if possible and single out the specific data to which the restriction of rights applies, such as, the preliminary results of an investigation, a decision opening an inquiry etc.
50. **The scope** of the restrictions should be specified, this is, which rights are concerned and how far they are going to be limited. It could be specified for instance that the restriction will only concern access rights or alternatively that it may concern access, rectification and confidentiality of communication.
51. **The safeguards should be indicated**, this is, measures that the controller is going to put in place in order to prevent abuse or unlawful access or transfer. This refers in particular to organisational and/or technical measures necessary to avoid breaches or unlawful transfers. It may also concern periodic measures to review a given decision on restriction. Each of the restrictions should be reviewed every six months to ensure that the grounds that justify it are still valid. For instance, it could be specified that in case of an electronic document there will be a double password, or that in case of physical documents they may be stored in a safe.

---

<sup>35</sup> A consultation will have to send to the functional mailbox of the EDPS: [edps@edps.europa.eu](mailto:edps@edps.europa.eu)

52. **The specification** of the controller or categories of controllers will have to be mentioned. As a matter of principle, it is recommended to refer to the function of the person instead of the names<sup>36</sup>.
53. **The storage periods** will have to be mentioned; this means that a retention period should be indicated. For instance, the retention period could be as long as the processing operation is necessary and some additional time could also be established for potential litigation.
54. Finally **the risk to the rights** and freedoms of the data subject will have to be analysed and specified such as those concerning right of defence, information etc.

## 6. Information about restrictions

### 6.1 General information

55. Data subjects need to be informed on a general basis that a restriction may apply to them (Annex III). For this purpose, a general data protection notice should always be posted in intranet/extranet of the EUI. For example, for transparency reasons, data subjects need to know that if an OLAF or an IDOC investigation applies to them, there is a certain period during which they could not even know that this is the case. They should also know that other rights may be restricted during this period. As the WP 29 has put it ‘data subjects should not be taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against a controller’<sup>37</sup>. The data subject should know about the purpose of the processing operation and the right to lodge a complaint with the EDPS. Still if the data subject asks for any of their right during this stage, the controller could refer to the general data protection notice.
56. At a later stage, for instance, when the preliminary phase of the investigation or inquiry has finished, data subjects should receive a (specific) data protection notice. Still at this point in time one cannot exclude that some rights have to be restricted, such as the right of access to the documents opening an investigation, or the documents containing allegations of the potential victims of a harassment. This fact should be indicated in the data protection notice and if possible also an indication of the time in which the rights will be fully restored.
57. It has been stated before that a restriction does not mean a denial of rights. For this reason as soon as the circumstances that justified the restriction are finished, the data subject will have the right to know that there has been a restriction. This is to be done in the form of a specific data protection notice that will be adapted to each case scenario and thus to each data subject concerned by the restriction.

---

<sup>36</sup> The reasons are obvious, given that the function stays but the person could leave the service and be replaced.

<sup>37</sup> See paragraph 68 of the WP 29 Guidelines on transparency under Regulation 2016/679 adopted on 29 November 2017, footnote 13.



## 6.2 Specific cases

58. In accordance with Articles 25 (6) to (8) of the new Regulation, the controller has to inform the data subject about the principal reasons for the restriction as well as his or her right to lodge a complaint to the EDPS unless doing so would cancel the effect of the restriction.
59. The general principle is thus that the data subject to which a restriction is imposed should be informed of the principal reasons of the restriction as well as his or her right to lodge a complaint to the EDPS. In some cases, it could be argued that the general data protection notice published in the intranet/extranet of the EUI plays a role on informing on the restriction. In other cases the data subject may directly request access to his personal data, rectification or other and then the controller should in principle inform the data subject of the main reasons for the restriction (such as to protect an investigation, to protect a witness, etc.) as well as his or her right to lodge a complaint to the EDPS.
60. There may be cases in which a data subject directly asks for a right at a very delicate moment of a given investigation; in those cases, if possible, the data subject will be informed of the main reasons of the restriction. Nevertheless, in other cases informing the data subject of the principal reasons of the restriction can result in cancelling the effect of the restriction – we cannot inform that we are investigating you because this would hamper the preliminary effects of our investigation- and in these cases, if properly justified, the information as to the main reasons of the restriction and the right to lodge a complaint to the EDPS can be deferred, omitted or denied for the sake of guaranteeing the effect of the restriction as such.
61. In other words, in extraordinary circumstances, for instance in the very preliminary stages of an investigation, if the data subject requests information if he or she is being investigated, the controller could decide not to grant at that moment that information - if this restriction is allowed under its internal rules and strictly necessary in the specific case; but also the controller could decide to, for instance, defer the information to be given to the data subject on the main reasons for such restriction and on his or her right to lodge a complaint before the EDPS, as any response would cancel the effect of the restriction imposed.
62. In cases where a restriction is imposed and the data subject is informed on the main reasons for the application of the restriction (for instance to safeguard the investigation we cannot give you access yet) he or she will be informed of her right to lodge a complaint with the EDPS. The role of the EDPS will be to inform the data subject if the data have or have not been processed correctly (if it is not the case whether the necessary corrections have been made).

## 7. Conclusion

63. Data protection is an EU fundamental right that encompasses several rights such as the right of access, to rectification, right of erasure etc. Scrupulous compliance with these rights is necessary to safeguard the essence of the right to data protection. It is within this framework that restrictions to the fundamental right may apply; restrictions are

exceptions to the rule and as such they have to be both justified under the necessity and proportionality test and documented. The internal rules should reflect this needs.

## ANNEX I: Article 25 of the Regulation

### Article 25

#### Restrictions

1. Legal acts adopted on the basis of the Treaties or, in matters relating to the operation of the Union institutions and bodies, internal rules laid down by the latter may restrict the application of Articles 14 to 22, 35, and 36, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
  - (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.
2. In particular, any legal act or internal rule referred to in paragraph 1 shall contain specific provisions, where relevant, as to:
  - (a) the purposes of the processing or categories of processing;
  - (b) the categories of personal data;
  - (c) the scope of the restrictions introduced;
  - (d) the safeguards to prevent abuse or unlawful access or transfer;
  - (e) the specification of the controller or categories of controllers;

- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; and
- (g) the risks to the rights and freedoms of data subjects.

[.....]

5. Internal rules referred to in paragraphs 1, 3 and 4 shall be clear and precise acts of general application, intended to produce legal effects vis-a-vis data subjects, adopted at the highest level of management of the Union institutions and bodies and subject to publication in the Official Journal of the European Union.
6. If a restriction is imposed pursuant to paragraph 1, the data subject shall be informed in accordance with Union law 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 European Data Protection Supervisor.
7. If a restriction imposed pursuant to paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.
8. Provision of the information referred to in paragraphs 6 and 7 of this Article and in Article 45(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1 of this Article.

## ANNEX II: Model of internal rules

DECISION .../...

of XXX

**on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of [administrative inquiries/ disciplinary proceedings/ investigations/ other] carried out by the [insert name of EUI]**

[THE EUI]

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,

Having regard to the opinion of the EDPS,

Whereas:

- (1) The [EUI] was set up by [decision] of [...] and its functions are [...];
- (2) The [EUI] [conducts administrative inquiries/disciplinary proceedings/internal investigations] [notifies cases to OLAF implying processing of personal data] [notifies cases to IDOC implying processing of personal data] [ conducts investigations] [conducts inspections ];
- (3) The [EUI] processes several categories of personal data [particularly identification data, contact data, professional data,]. The [EUI], represented by its Director-General, acts as the data controller. The personal data are stored in a secured electronic environment which prevents unlawful access or transfer of data to persons who do not have a need to know. The personal data processed are retained [for fifteen years after the case is dismissed or the investigation or the coordination case is closed by a decision of the Director-General. At the end of the retention period, the case related information including personal data is transferred to the historical archives];
- (4) The internal rules should apply to all processing operations carried out by the [EUI] in the performance of its [please specify the ground(s) for the restriction]. They should apply to processing operations carried out prior to the opening of an [please specify the scope: investigation/ both during internal and external investigations/during the monitoring of the follow-up to the outcome of the investigations]. The rules should apply to processing operations which form part of the activities linked to the [please specify the scope, for example investigative function such as [...]]. It should also include assistance and cooperation provided by the Office to national authorities and international organisations outside of its administrative investigations;

- (5) The [EUI] 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;
- (6) Within this framework [EUI] 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 access and rectification, right to erasure, data portability etc. as enshrined in Regulation (EU) No 2018/1725;
- (7) However, [the EUI] may be obliged to defer 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/other];
- (8) The [EUI] may thus defer the information for the purpose of [protecting the investigation/other];
- (9) The [EUI] should lift the restriction as far as the conditions that justify the restriction no longer apply;
- (10) The [EUI] should monitor the conditions on a regular basis [every month] [every three months] [every six months] [other]<sup>38</sup>;
- (11) The [EUI] should consult the DPO [at the moment of deferral/during the revisions/every three months],

HAS ADOPTED THIS DECISION:

*Article 1*  
*Subject-matter and scope*

1. This Decision lays down rules relating to the conditions under which the [EUI] in the framework of [administrative inquiries/disciplinary proceedings/internal investigations/other] may restrict the application of the rights enshrined in Articles 14 to 22, 35 and 36, as well as Article 4 thereof, following Article 25 of the Regulation (EU) No 2018/1725.
2. This Decision applies to the processing operation of personal data by the [EUI] for the purpose of [conducting investigations/ administrative inquiries and/or disciplinary proceedings/other].
3. The categories of data concerned are [hard data (administrative details, telephone, private address, electronic communications, and traffic data) and/or soft data

---

<sup>38</sup> Longer than six months will apply only in very exceptional circumstances.

(appraisals, opening of inquiries, reports on preliminary investigations) etc.].

4. Subject to the conditions set out in this Decision, the restrictions may apply to the following rights: [access and rectification rights/access, rectification, erasure and portability/ rights of information/ confidentiality of communication/ principles of the data processing operation provided that they relate to a right/others]

## *Article 2*

### *Specification of the controller and safeguards*

1. The safeguards in place to avoid data breaches, leakages or unauthorised disclosure are the following: [double passwords, safes, others]
2. The controller of the processing operation is [please specify the function]<sup>39</sup>
3. The storage or retention period of the [categories of data] is the following [please insert a period that is not longer than necessary for fulfilment of the purpose and eventually to allow judicial or administrative disputes]
4. The risk to the rights and freedoms of the data subject is the following [...]

## *Article 3*

### *Restrictions*

1. Any restriction shall only be applied to safeguard [please specify which ground(s) under Article 25(1) of Regulation 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;

---

<sup>39</sup> In principle the name should not be specified, only the function.

- (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.
2. Any restriction shall be necessary and proportionate in a democratic society and respect the essence of the fundamental rights and freedoms.
  3. 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.
  4. Restrictions shall be duly monitored and a periodical revision shall be done every [month] [three months] [six months].
  5. Restrictions shall be lifted as soon as the circumstances that justify them no longer apply. [please specify as far as possible such circumstances already in the internal rules].

#### *Article 4*

##### *Review by the Data Protection Officer*

1. The [EUI] shall, without undue delay, inform the Data Protection Officer of the [EUI] ("the DPO") whenever it restricts the application of data subjects' rights in accordance with this Decision and shall provide access to the record and the assessment of the necessity and proportionality of the restriction.

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

#### *Article 5*

##### *Provision of information to data subject*

1. The EUI shall include in the data protection notices published on its website 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. Additionally, the EUI shall inform individually data subjects on their rights concerning present or future restrictions without undue delay and in a written form, without prejudice of the following paragraph.
3. Data subjects shall be informed on the principal reasons on which the application of a restriction is based and of their right to lodge a complaint before the European Data Protection Supervisor. [as the case may be, specify the cases where the information would cancel the effect of the restrictions imposed and specify whether it will therefore be deferred, omitted or denied].

#### *Article 6*

##### *Right of access by data subject*

(...)[if applicable. The EUI should adopt one Article per personal data right to be restricted]

#### *Article 7*

##### *Right of [...]*

(...)[if applicable. The EUI should adopt one Article per personal data right to be restricted]

#### *Article 8*

##### *Entry into force*

This Decision shall enter into force on [*the day of entry into force of Regulation (EU) No 2018/1725*] [*other*].

## ANNEX III: Internal note on a concrete restriction- Necessity and proportionality test model.

Case file number:

The controller, on the basis of the following:

Regulation No 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<sup>40</sup>, in particular its Article 25,

EUI internal rules published in the OJ on [.....],

The consultation of the Data Protection Officer on [.....],

The [confidential/restricted] note of .... dated..... which [opened an inquiry/decided to send a case to OLAF/ decided to send a case to IDOC/opened an internal investigation] on the person/on case.....<sup>41</sup>,

[Insert a short description of the main purpose for the processing of personal data]

On the basis of the following reasons as stated in Article 25 (1) of Regulation No 2018/1725: [the national security, public security or defence of the Member States] [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] [others],

The necessity for doing so is the following [.....] and proportionality of the measure has been assessed as follows [..... specify the risks to the rights and freedoms of data subjects taken into account]

The reasons for the restriction and its duration are the following: [explain briefly the background.....]

Deems necessary to restrict the following right[s] of the data subjects: [specify the rights from Articles 14 to 22, 35, and 36 of Regulation No 2018/1725, as well as its Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22], in relation to the following categories of data:

---

<sup>40</sup> OJ L 295, 21.11.2018, p. 39.

<sup>41</sup> If applicable.

The duration of the restriction is of [1 month/ 3 months/6 months].

[The restriction has been revised, in consultation with the Data Protection Officer on [every six months as of the date of signature].]

Signed.....

## ANNEX IV: Model – Extract of General Data Protection Notice informing on the possible restrictions<sup>42</sup>

The purpose of the present processing operation is to [send information on data subjects to OLAF] [send information on data subjects to IDOC] [open an internal administrative procedure on a data subject] [open an investigation] [other purpose]

Within this context, you have the rights of access, rectification, right to erasure, to restriction of processing, of notification in case of rectification or erasure or restriction of processing and right to data portability. A breach concerning your personal data shall be communicated to you under certain circumstances. The institution shall also ensure the confidentiality of electronic communications.

Nevertheless, you should be informed that by virtue of Article 25 of Regulation No 2018/1725 and of the Internal Rules laid down under Decision<sup>43</sup> ... , one or several of these rights may be restricted for a temporary period of time *inter alia* on the grounds of prevention, investigation, detection and prosecution of criminal offences [or other ground]. Any such restriction will be limited in time, proportionate and respect the essence of the above-mentioned rights. It will be lifted as soon as the circumstances justifying the restriction are no longer applicable. You will receive a more specific data protection notice when this period has passed.

As a general rule you will be informed on the principal reasons for a restriction unless this information would cancel the effect of the restriction as such.

You have the right to make a complaint to the EDPS concerning the scope of the restriction.

---

<sup>42</sup> To be posted generally on internet.

<sup>43</sup> published in the OJ .. on ...