EUROPEAN DATA PROTECTION SUPERVISOR

Guidance on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects rights

Updated: 24 June 2020

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 strictly respected. However, according to EU secondary legislation they could be restricted in exceptional circumstances and with the safeguards laid down in Regulation (EU) 2018/1725. The EU institutions, bodies and agencies should adopt such restrictions only where strictly necessary and always based on a legal act or, in the absence of such a legal act, on internal rules adopted by the highest level of management and published in the Official Journal of the European Union.

Restrictions carried out on the basis of internal rules are only possible in matters relating to the operation of the EU institutions, bodies and agencies. Each restriction should be linked to the applicable legal grounds for restricting an individual's (data subject) rights as provided for in Article 25(1) of the Regulation. Consulting the EDPS when drawing up internal rules is required.

On the basis of the internal rules and for accountability purposes, the data controller should draft a 'proportionality and necessity test' which assesses 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 during the entire process.

This guidance focuses on the conditions under which internal rules may restrict these rights, how to draft such rules and how to interpret and apply restrictions in specific cases. The EDPS updated this guidance drawing on best practice across the EU institutions, bodies and agencies since the Regulation's entry into force.

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 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 ('DPO') when drawing up internal rules;

R6: Consult the European Data Protection Supervisor ('EDPS') when drawing up internal rules;

R7: Review your internal rules periodically and 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: Inform data subjects using a general data protection notice which includes information 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 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[1];

R7: Document restrictions for accountability purposes;

R8: Monitor your restriction on a regular basis.

[1] The controller should involve the DPO throughout the procedure and document this consultation.

Checklist – Specific provisions to be included in internal rules governing restrictions of data subject rights

In accordance with Article 25(2), internal rules governing the restrictions should, where appropriate, contain the following specific provisions as to:

- ✓ the **purposes** of the processing or categories of processing (i.e. the need to open administrative inquiries or disciplinary proceedings);
- ✓ the **categories of personal data** (the categories of data affected by restrictions should be specified);
- ✓ the **scope** of the restrictions introduced (it should be specified which rights are concerned and how far they are going to be limited);
- ✓ the **safeguards** that the controller is going to put in place in order to prevent abuse or unlawful access or transfer;
- ✓ the specification of **the controller** or categories of controllers;
- ✓ the **storage periods** taking into account the nature, scope and purposes of the processing or categories of processing;
- ✓ assessment of the **risks to the rights and freedoms of data subjects**.

In addition:

- ✓ check cases where your EU Institution has applied restrictions in the past, to identify the needs your internal rules must meet;
- ✓ make sure that each processing operation for which you need to restrict data subject rights is clearly linked to a legal ground for restriction under Article 25 of the Regulation;
- ✓ consult the EDPS in a timely manner, in order to be able to change the draft internal rules before their final approval, if necessary;
- ✓ inform the relevant units and/or departments on how to deal with restrictions of data subject rights.

TABLE OF CONTENTS

1. Introduction

1. Fundamental rights and freedoms are at the core of EU democracies. The EDPS has a duty to ensure that the work of the European Union institutions, agencies, offices and bodies ('EUIs') is guided by a respect for the protection of fundamental rights and freedoms of individuals in relation to the processing of personal data. The processing of personal data should be designed to serve humankind[2] 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 ('Charter'). Regulation (EU) 2018/1725 (the 'Regulation')[3] contains those rights and complements them with a number of additional rights, some were already provided for to a large extent in Regulation 45/2001[4], such as the right to object and erasure[5], and others are new, such as the right to portability.

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 Regulation should be read and interpreted. This provision is entitled 'restrictions' and it states that in the situations that are listed in it, EUIs may restrict the application of certain provisions of the Regulation, mainly relating to the rights of the data subjects. **Restrictions are exceptions to the general rule and, as such, should be applied only in limited circumstances. If any are applied, then the controller should be in a position to justify and explain its course of action.**[6].

4. According to Article 52(1) of the Charter[7], any limitation on the exercise of the rights and freedoms recognised by the Charter must be 'provided for by law'. This corresponds to the

[2] 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, page 1.

[3] 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, page 39.

[4] 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, page 1.

[5] This right is also called the 'right to be forgotten'.

[6] A restriction is different from an exception, such as those mentioned in Article 16(5).

[7] 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, 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.'

expression 'in accordance with the law' in Article 8(2) of the European Convention of Human Rights (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[8]. The same strict standard should be applied 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 Regulation provides nonetheless that, in matters relating to the operation of EUIs, restrictions may be provided for by internal rules. Therefore, **in general, restrictions should be provided for by legal acts; in cases where there is no legal act but where necessity is proven, restrictions may be provided for by internal rules.**

5. **This guidance explains when the EUIs may apply restrictions and how to draft internal rules that constitute the legal basis for such restrictions**[9]. 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 EU legal act or, in matters relating to the operation of an EUI, by fully-fledged internal rules adopted at the highest level of the EUI. **Therefore, this is a new development since 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'[10]. 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 so as 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 extensive and intrusive to the extent that they void a fundamental right of its basic content, cannot be justified. If the essence of the right is compromised, the limitation must be considered unlawful, without the need to further

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

[9] 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 Regulation).

[10] https://en.oxforddictionaries.com/definition/restriction

assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria[11].

8. The EDPS Necessity Toolkit has provided that there must be an assessment of 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[12].

3. Which rights may be affected by a restriction?

9. The data subject rights and EUI obligations that may be restricted under Article 25(1) are exclusively those provided for by **Articles 14 to 22 of the Regulation** as well as Articles **35 and 36** of the Regulation and **Article 4** insofar as their provisions correspond to the rights and obligations provided for in Articles 14 to 22.

10. 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 scenarios (when data were collected from the data subjects and when data were not collected from them respectively)[13]. This restriction should not apply to general data protection notices that include information about the possibility to restrict information for a period of time (for a model see Annex IV). This is to ensure compliance with the principle of fairness. The Working Party 29 (WP29) 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'[14].

11. 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 so as not to hamper the preliminary steps of the inquiry. This applies also to a decision of the European

---

[11] 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 Kärntner Landesregierung and Others.

[12] See page 4 of the EDPS 'Necessity Toolkit': https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[13] Concerning transparency and information to data subjects, see the 'Guidance paper Articles 14-16 of the new regulation 45/2001 transparency rights and obligations' : https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf

[14] 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).

Anti-Fraud Office (OLAF) to open an investigation or for the transmission of a case to OLAF. The right to rectification, for instance, may be restricted during this type of investigation.

12. The application of **Article 19** on the right to erasure (also called the 'right to be forgotten') can be restricted. This right often applies when there is an issue with the lawfulness of a 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 erased.

13. **Article 20** is about the right to restriction of processing and **Article 21** about the need to notify any restriction of processing carried out in accordance with Article 20 as well as any rectification and erasure. The right to restriction of processing is the former right to have data blocked.

14. **Article 22** concerns the right to data portability. While the Regulation provides for the possibility to restrict the right to data portability, EUIs should keep in mind that its scope of application is limited. This right *only* applies when the lawful basis for processing this information is consent (Article 5(1)(d)) or the performance of a contract (Article 5(1)(c) and when carrying out the processing by automated means. Conversely, it does not apply to processing carried out in the performance of a task in the public interest based on law (Article 5(1)(a)) and the other grounds for lawfulness in Article 5. Since Article 5(1)(a) is the most common ground for lawfulness of processing in the EUIs, the scope of the right to data portability is rather narrow in the EUIs. It is possible that your EUI does not carry out any processing operations to which the right to portability applies. Where this right does not apply in the first place, there can logically be no need to restrict it. When drafting their internal rules, EUIs should check if they (1) carry out processing operations to which the right to data portability applies and (2) whether there is a justified need under Article 25(1) to restrict this right. If the answer to either question is 'no', then do not include the possibility to restrict the right to portability in your internal rules, because it is not applicable anyway.

15. **Article 23** concerns the right to object. It is important to note that the right to object cannot be restricted under Article 25(1)[15]. The data subject always has a right to object to the 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[16].

---

[15] This right allows data subjects to object to lawful processing on grounds relating to their particular situation.

[16] 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.'

16. **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[17]. Given that a restriction to the confidentiality of electronic communications may interfere with the essence of the right to privacy, it is only in extraordinary circumstances that this right can be restricted[18].

17. In addition, a restriction 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 consequently 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 EU 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 assessed whether an accessible and foreseeable **law provides for a limitation**, and whether **the essence of the right is respected**[19]. The following test is to see 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

---

[17] See the Guidelines of February 2020 on personal data and electronic communications in the EU institutions (eCommunications guidelines): https://edps.europa.eu/sites/edp/files/publication/20-01-31_guidelines_on_electronic_communications_en.pdf

[18] Accordingly, any restriction of this right would have to correspond to the high standards laid down in 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, page 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]). EUIs should be especially careful regarding any restriction to the confidentiality of electronic communications without properly informing data subjects, which should not take place outside of the strict justifying scenario identified in the necessity and proportionality assessment (see further down). See also EDPS Guidelines on Data Breaches published on 11 December 2018.

[19] See paragraph 8 of this guidance paper.

allow the assessment on whether the measure is necessary[20]. The next step is to **assess the necessity of the envisaged restrictions.** The case law of the Court of Justice of the European Union (CJEU) 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 insofar 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[21].

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[22].

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 Regulation, any restriction has to be either based on a legal act adopted on the basis of the Treaties or, in the absence of such legal basis, in matters relating to the operation of EUIs, on the internal rules of the EUIs. This is different from the previous Regulation[23], where restrictions were based on Article 20 directly.

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 that they are published in the Official Journal of the European Union. This guidance focuses 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, meaning restrictions cannot be carried out under any other conditions than the ones listed 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

---

[20] For more information on this, see section 4.3. of this guidance paper on the grounds for restricting.

[21] For further guidance on how to apply the necessity test, please refer the EDPS 'Necessity Toolkit' ('Assessing the necessity of measures that limit the fundamental right the protection of personal data: A Toolkit'): https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

[22] For further guidance on how to apply the proportionality test, please refer to the EDPS 'Proportionality Toolkit' ('Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data'): https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf

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

perform a *necessity and proportionality test* on the restriction that it intends to apply. In other words, the controller should document why its restriction is necessary, as well as how it intends to comply with the requirement of not restricting more than is necessary[24].

26. The controller should revise said note when necessary (Annex III); 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 rights can have national or public security and/or defence of the Member States as a basis. Restrictions based on national security have often been associated with surveillance and processing of data for intelligence purposes[25].

28. Moreover, public security includes protection of human life, especially in response to natural or manmade disasters. In addition, EUIs could 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'[26]. The 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 or 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

---

[24] See WP 29 Opinion on some key issues of the Law Enforcement Directive, adopted on 29 November 2017. Although limited to law enforcement, point 4 on limitations to the right of access, in the 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 mentioned in footnote 12.

[25] 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 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.'

[26] 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, page 53, provides that access rights of data subjects may be restricted to 'guarantee that any national investigation will not be jeopardised'.

investigation. The same applies for EUIs that notify cases to the 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, there is a certain period of time when rights can be restricted[27].

31. The EDPS recognises that 'providing information to the data subject while the investigation is still ongoing could jeopardise the success of said investigation…'[28] The omitted information must, in accordance with the case law of the CJEU, be provided once it is no longer possible for it to jeopardise the investigation being carried out[29]. This means that a specific (tailor-made) data protection notice must be given to the data subject as soon as possible, 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.'[30]

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 a formal procedure has been initiated. In particular, if there are connections with criminal offences it is 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 on their websites informing potential data subjects on the potential temporary restriction of their rights (see Annex IV). EUIs should also draft specific data protection notices once it is no longer possible for access and other rights to jeopardise the investigation being carried out.

---

[27] In the Guidelines on the rights of individuals with regard to processing of personal data issued under Regulation 45/2001, 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.

[28] See Guidelines mentioned above, page 28.

[29] Opinion 1/15 of the CJEU (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017.

[30] See joint cases 2010-0797, 2010-0798 and 2010-0799.

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 has 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 the submission of application for 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 EU.

4.3.4 The internal security of Union institutions and bodies, including 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 grounds 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.

4.3.5 The protection of judicial independence and judicial proceedings

35. Any restriction of this kind could be applied by the CJEU 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 inquiries 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, certain cases of harassment, conflict of interests etc. These are cases in which an investigation is carried out by the institution, IDOC (or potentially by OLAF) but there is no connection in principle with criminal offences as, in that case, point 4.3.2 would be applicable. This being said, the difference between these cases and those stated in point 4.3.2 may not always be clear-cut, so in case of doubt both legal bases could be used for a given restriction.

37. As 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 harassers to

their own data[31]. The reason is of course for the protection of the alleged victim. The right of access of the alleged harassers depends on the information that they have; they will not request access if they are not aware of an existing informal procedure involving them. 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 if only 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 Regulation

38. This restriction refers to a potential limitation when there is an inspection or a monitoring exercise or a regulatory function connected, even if only occasionally, to the exercise of official authority in the cases referred to in points 4.3.1 to 4.3.3., performed by an EUI. It could be the case in a targeted audit, for instance, or an inspection in the framework of an investigation. In these cases, a general data protection notice should nevertheless be given to the data subject or posted on the internet/intranet of the EUI. As an example, during an audit of a recruitment procedure of a member of staff, 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 whistleblowers 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 service of an EUI, in order to restrict access to medical data of a psychological or psychiatric nature. Given the potential sensitivity of some of these data, the medical service of the institution may want to give the data subjects indirect access through their own practitioner.

4.3.9 The enforcement of civil law claims

This rule comes from the GDPR and it seems to fit more within a national context. In any case, it is a new ground to apply a restriction which did not appear in the previous regulation.

5. How to draft internal rules and implement them

5.1 The principles

41. Internal rules should be **clear and precise and for general application**. A model is provided in this Guidance document (Annex II) 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 advised that the EUI identify which (categories of) processing operations need to be covered by the internal rules. In general, a necessity test on the need to apply restrictions should also be performed - this is the question of

[31] See EDPS case 2011-0483.

'does our EUI have a need to be able restrict data subject rights here?'[32]. Even if the answer is 'yes' on this general level, each instance in which an EUI uses those restrictions should be justified on a case-by-case basis (see Article 2(4) in ANNEX II: Model of internal rules).

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 also be 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 on the intranet and website of the institution.

44. On the basis of Article 41 (2) of the Regulation, the EDPS should be consulted when the EUI is drawing up the internal rules[33].

45. On the basis of these rules, each time an EUI needs to impose a restriction it should first carry out a 'necessity and proportionality test' that must be duly documented (see Annex III). This assessment could either be carried out 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 containing specific provisions on a number of issues outlined in the following paragraphs.

48. The internal rules should refer to the **purpose of the processing or categories of processing,** such as the need to open administrative inquires or disciplinary proceedings, notification of cases to OLAF, the need to conduct investigations, etc.

49. The rules should refer to **categories of personal data to which restrictions will apply.** Where possible, the controller can go further and list the specific data items to which the

[32] For further information on how to conduct this necessity test, see the EDPS Necessity Toolkit referred to in footnote 12.

[33] A consultation will have to be sent to the functional mailbox of the EDPS: edps@edps.europa.eu

restriction of rights may apply, such as the preliminary results of an investigation, a decision opening an inquiry, etc.

50. **The scope** of the restrictions should also be specified, i.e. which rights are concerned and how far they are going to be limited, for instance, the restriction will only concern access rights, or alternatively that it may concern access, rectification and confidentiality of communication.

51. As far as possible, the internal rules should link the processing operation, the categories of personal data concerned, the scope of the restrictions and the rights that will be restricted. For example, possible restrictions of the right of access to data for alleged harassers in anti-harassment procedures, where this is necessary to protect other persons.

52. **Safeguards should be indicated** in the internal rules. These safeguards are the measures that the EUI 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 which are necessary in order to avoid breaches or unlawful transfers such as the storage in a safe of physical documents. It may also concern periodic measures to review a given decision on restrictions. Each restriction should be reviewed every six months to ensure that the justification for it is still valid.

53. **Specify who** the controller is or list the categories of controllers. The EDPS recommends that a reference is made to the function of the person rather than listing the names[34].

54. **The storage or retention period** should be indicated. For instance, the retention period could be calculated as the duration of the processing operation plus additional time for potential litigation.

55. **The risk to the rights** and freedoms of the data subject should be analysed and specified, such as those concerning the right of defence, information etc.

6. Information about restrictions

6.1 General information

56. Data subjects must be informed that a restriction may apply to them (Annex IV). For this purpose, a general data protection notice should always be posted on the intranet and website of the EUI. For example, for transparency reasons, data subjects should be aware that if they are implicated in an OLAF or an IDOC investigation, there will be a certain period during which they might not be aware of it. They should also know that other rights might be restricted during this period. 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[35]. The data subject should know about the purpose of the processing

[34] The reasons are obvious, given that the function stays but the person could leave the service and be replaced.

[35] See paragraph 68 of the WP 29 Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, referred to in footnote 14.

operation and the right to lodge a complaint with the EDPS. In any case, if the data subject requests to exercise any of their rights during the preliminary phase of the investigation, the controller can refer to the general data protection notice.

57. At a later stage, such as after the preliminary phase of the investigation or inquiry is completed, data subjects should receive a (specific) data protection notice, for example by email. It is still possible at this stage that certain rights will continue to be restricted, such as the right of access to the documents opening an investigation, or the documents containing the allegations of potential victims of harassment. This fact should be indicated in the data protection notice along with an indication of a period in which the rights will be fully restored, if possible.

58. A restriction is not a denial of rights. For this reason, once the circumstances that justified the restriction are no longer valid, the data subject has the right to know that a restriction was in place. This is to be done in the form of a specific data protection notice, adapted for each scenario and each data subject concerned by the restriction.

6.2 Specific cases

59. In accordance with Articles 25 (6) to (8) of the Regulation, the controller has to inform the data subject about the principal reasons for the restriction as well as their right to lodge a complaint with the EDPS, unless doing so would cancel the effect of the restriction.

60. The general principle is that the data subject on which a restriction is imposed should be informed of the principal reasons of the restriction as well as their right to lodge a complaint to with the EDPS. In some cases, the general data protection notice published on the intranet/website of the EUI is sufficient information to data subjects about the restrictions. In other cases, the data subject may have a direct request regarding their personal data, in which case 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 their right to lodge a complaint with the EDPS.

61. Where a data subject specifically asks to exercise a particular right at a very delicate moment of a given investigation, the data subject should, if possible, be informed of the main reasons for the restriction. However, if informing the data subject of the principal reasons for the restriction would result in cancelling the effect of the restriction (i.e. would hamper the preliminary effects of the investigation), then the information about the main reasons for the restriction and the right to lodge a complaint with the EDPS can be deferred, omitted or denied for the sake of guaranteeing the effect of the restriction, if properly justified.

62. 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; the controller could also decide to defer the information to be given to the data subject on the main reasons for such restriction and on their right to lodge a complaint before the EDPS, as any response would cancel the effect of the restriction imposed.

63. In cases where a restriction is imposed and the data subject is informed of the main reasons for the application of the restriction (e.g. “to safeguard the investigation we cannot give you access yet”) they must also be informed of their right to lodge a complaint with the EDPS. The role of the EDPS will be to inform the data subject if their data have or have not been processed correctly (and if they have not been processed correctly, whether the necessary corrections have been made).

7. Conclusion

64. Data protection is an EU fundamental right that encompasses several rights such as the right of access, to rectification, right to erasure etc. Strict 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 these requirements.

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

[only keep the parts relevant to your EUI; situations not covered by the model to be added, if necessary]

DECISION …/…

of [EUI] of [date]

on internal rules concerning restrictions of certain data-subject rights in relation to the processing of personal data in the framework of activities carried out by the [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[36], and in particular Article 25 thereof,

Having consulted the European Data Protection Supervisor,

Whereas:

(1) The [EUI] is empowered to conduct administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings, in accordance with the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ('Staff Regulations')[37], and with the [EUI] Decision of [date] adopting implementing provisions regarding the conduct of administrative inquiries and disciplinary proceedings. If required, it also notifies cases to OLAF.

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

(3) The [EUI] has put in place a policy to prevent and deal effectively with actual or potential cases of psychological or sexual harassment in the workplace, as provided for in its Decision of [date] adopting implementing measures pursuant to the Staff Regulations.

---

[36] OJ L 295, 21.11.2018, p. 39.

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

The Decision establishes an informal procedure whereby the alleged victim of the harassment can contact the [EUI]'s 'confidential' counsellors.

(4) The [EUI] can also conduct investigations into potential breaches of security rules for European Union classified information ('EUCI'), based on its Decision of [date] amending/adopting its security rules for protecting EUCI.

(5) The [EUI] is subject to both internal and external audits concerning its activities.

(6) In the context of such administrative inquiries, audits and investigations, the [EUI] cooperates with other Union institutions, bodies, offices and agencies.

(7) The [EUI] can cooperate with third countries' national authorities and international organisations, either at their request or on its own initiative.

(8) The [EUI] can also cooperate with EU Member States' public authorities, either at their request or on its own initiative.

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

(10) To fulfil its tasks, the [EUI] collects and processes information and several categories of personal data, including identification data of natural persons, contact information, professional roles and tasks, information on private and professional conduct and performance, and financial data. The [EUI] acts as data controller.

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

(12) The [EUI] might be required to reconcile those rights with the objectives of administrative inquiries, audits, investigations and court proceedings. It might also be required to balance a data subject's rights against the fundamental rights and freedoms of other data subjects. To that end, Article 25 of the Regulation (EU) 2018/1725 ('the Regulation') gives the [EUI] the possibility to restrict, under strict conditions, the application of Articles 14 to 22, 35 and 36 of the Regulation, as well as its Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 20. Unless restrictions are provided for in a legal act adopted on the basis of the Treaties, it is necessary to adopt internal rules under which the [EUI] is entitled to restrict those rights.

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

need to protect the rights and freedoms of witnesses as well as those of other persons involved.

(14) It might be necessary to protect the anonymity of a witness or whistle-blower who has asked not to be identified. In such a case, the [EUI] might decide to restrict access to the identity, statements and other personal data of such persons, in order to protect their rights and freedoms.

(15) It might be necessary to protect confidential information concerning a staff member who has contacted [EUI] confidential counsellors in the context of a harassment procedure. In such cases, the [EUI] might need to restrict access to the identity, statements and other personal data of the alleged victim, the alleged harasser and other persons involved, in order to protect the rights and freedoms of all concerned.

(16) The [EUI] should apply restrictions only when they respect the essence of fundamental rights and freedoms, are strictly necessary and are a proportionate measure in a democratic society. The [EUI] should give reasons explaining the justification for those restrictions.

(17) In application of the principle of accountability, the [EUI] should keep a record of its application of restrictions.

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

(19) Article 25(6) of the Regulation obliges the controller to inform data subjects of the principal reasons on which the application of the restriction is based and of their right to lodge a complaint with the EDPS.

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

(21) The [EUI] should lift the restriction as soon as the conditions that justify the restriction no longer apply, and assess those conditions on a regular basis.

(22) To guarantee utmost protection of the rights and freedoms of data subjects and in accordance with Article 44(1) of the Regulation, the DPO should be consulted in due time of any restrictions that may be applied and verify their compliance with this Decision.

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

HAS ADOPTED THIS DECISION:

Article 1
Subject-matter and scope

1. This Decision lays down rules relating to the conditions under which the [EUI] may restrict the application of Articles 4, 14 to 22, 35 and 36, pursuant to Article 25 of the Regulation.
2. The [EUI], as the controller, is represented by [function at the highest management level].

Article 2

Restrictions

[only keep the relevant parts; other cases, not included on the list, to be added, if necessary]

1. The [EUI] may restrict the application of Articles 14 to 22, 35 and 36, and Article 4 thereof in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 20:

   (a) pursuant to Article 25(1) (b), (c), (f), (g) and (h) of the Regulation, when conducting administrative inquiries, pre-disciplinary, disciplinary or suspension proceedings under Article 86 and Annex IX of the Staff Regulations and the [EUI] Decision of [date], and when notifying cases to OLAF;

   (b) pursuant to Article 25(1)(h) of the Regulation, when ensuring that [EUI] staff members may report facts confidentially where they believe there are serious irregularities, as set out in the [EUI] Decision on internal rules concerning whistleblowing of [date];

   (c) pursuant to Article 25(1)(h) of the Regulation, when ensuring that [EUI] staff members are able to report to confidential counsellors in the context of a harassment procedure, as defined by the [EUI] Decision of [date];

   (d) pursuant to Article 25(1)(c), (g) and (h) of the Regulation, when conducting internal audits in relation to activities or departments of the [EUI];

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

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

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

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

(x) [...]

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

3. A necessity and proportionality test shall be carried out on a case-by-case basis before restrictions are applied. Restrictions shall be limited to what is strictly necessary to achieve their objective.

4. For accountability purposes, the [EUI] shall draw up a record describing the reasons for restrictions that are applied, which grounds among those listed in paragraph 1 apply and the outcome of the necessity and proportionality test. Those records shall be part of a register, which shall be made available on request to the EDPS. The [EUI] shall prepare periodic reports on the application of Article 25 of the Regulation.

5. When processing personal data received from other organisations in the context of its tasks, the [EUI] shall consult those organisations on potential grounds for imposing restrictions and the necessity and proportionality of the restrictions concerned, unless this would jeopardise the activities of the [EUI].

Article 3
Risks to the rights and freedoms of data subjects

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

2. Whenever the [EUI] assesses the necessity and proportionality of a restriction it shall consider the potential risks to the rights and freedoms of the data subject.

Article 4
Safeguards and storage periods

1. The [EUI] shall implement safeguards to prevent abuse and unlawful access or transfer of the personal data in respect of which restrictions apply or could be applied. Such safeguards shall include technical and organisational measures and be detailed as necessary in [EUI] internal decisions, procedures and implementing rules. The safeguards shall include:

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

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

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

(d) due monitoring of restrictions and a periodic review of their application.

The reviews referred to in point (d) shall be conducted at least every six months.

2. Restrictions shall be lifted as soon as the circumstances that justify them no longer apply.

3. The personal data shall be retained in accordance with the applicable [EUI] retention rules, to be defined in the data protection records maintained under Article 31 of the Regulation. At the end of the retention period, the personal data shall be deleted, anonymised or transferred to archives in accordance with Article 13 of the Regulation.

Article 5

Involvement of the Data Protection Officer

1. The [EUI] DPO shall be informed without undue delay whenever data subject rights are restricted in accordance with this Decision. He or she shall be given access to the associated records and any documents concerning the factual or legal context.

2. The [EUI] DPO may request a review of the application of a restriction. The [EUI] shall inform its DPO in writing of the outcome of the review.

3. The [EUI] shall document the involvement of the DPO in the application of restrictions, including what information is shared with him or her.

Article 6

Information to data subjects on restrictions of their rights

1. The [EUI] shall include a section in the data protection notices published on its website/intranet providing general information to data subjects on the potential for restriction of data subjects' rights pursuant to Article 2(1). The information shall cover which rights may be restricted, the grounds on which restrictions may be applied and their potential duration.

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

3. The [EUI] may defer, omit or deny the provision of information concerning the reasons for a restriction and the right to lodge a complaint with the EDPS for as long as it would

cancel the effect of the restriction. Assessment of whether this would be justified shall take place on a case-by-case basis. As soon as it would no longer cancel the effect of the restriction, the [EUI] shall provide the information to the data subject.

Article 7

Communication of a personal data breach to the data subject

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

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

Article 8

Confidentiality of electronic communications

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

2. Where the [EUI] restricts the right to confidentiality of electronic communications, it shall inform the data subject concerned, in its reply to any request from the data subject, of the principal reasons on which the application of the restriction is based and of his or her right to lodge a complaint with the EDPS.

3. The [EUI] may defer, omit or deny the provision of information concerning the reasons for a restriction and the right to lodge a complaint with the EDPS for as long as it would cancel the effect of the restriction. Assessment of whether this would be justified shall take place on a case-by-case basis.

Article 9

Entry into force

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

Done at [location], [date].

For the [highest management level of the institution, body, agency]

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[38], 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……[39],

[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 the taken into account]

The reasons for the restriction and its duration are the following: [briefly explain 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, insofar as its provisions correspond to the rights and obligations provided for in Articles 14 to 22], in relation to the following categories of data:

[38] OJ L 295, 21.11.2018, page 39.

[39] If applicable.

The duration of the restriction is for [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 data subjects of possible restrictions[40]

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 will be communicated to you under certain circumstances. The institution should 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[41] ... , 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.

---

[40] To be posted on the EUIs intranet/website

[41] Published in the OJ .. on ...

ANNEX V: Glossary[42]

CONCEPT	DEFINITION
Personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law.
Data subject	The person whose personal data are collected, held or processed.

[42] Definitions in accordance with Article 3 of the Regulation. For further information consult the EDPS glossary available on its website: https://edps.europa.eu/data-protection/data-protection/glossary_en