EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on processing personal information within a whistleblowing procedure

July 2016

Executive Summary

Whistleblowing serves the purpose of shining the light on corruption. A key challenge to prevent and fight corruption is to detect and expose bribery, fraud, theft, and other acts of wrongdoing in the work place. Whistleblowing is a tool to make visibility to that kind of unethical behaviour.

Whistleblowers believe that they are acting in the public interest when reporting an activity observed of serious matter. Unfortunately whistleblowers commonly face retaliation in the form of harassment, firing, blacklisting, threats and their disclosures are routinely ignored. Confidentiality is therefore crucial and the most effective way to encourage staff to report concerns is to ensure them that their identity will be protected.

These Guidelines provides practical guidance to the EU institutions and bodies both before and after implementation of a whistleblowing procedure to ensure that they comply with the data protection obligations as set out in Regulation (EC) No 45/2001.

List of Recommendations

Below is a list of the recommendations detailed in the guidelines. The EDPS will use these as checklists in assessing your compliance with the obligations laid out in the Regulation.

1. Implement defined channels for internal and external reporting and specific rules where the purpose is clearly specified (p. 4-5).

2. Ensure confidentiality of the information received and protect the whistleblowers' identity and all other persons involved (p. 4-5).

3. Apply the principle of data minimisation: only process personal information, which are adequate, relevant and necessary, for the particular case (p. 6).

4. Identify what personal information means in this context and which are the affected individuals to determine their right of information, access and rectification. Restrictions to these rights are allowed, as long as the EU institutions are able to provide documented reasons before taking such a decision (p. 6-7).

5. Apply the two-step procedure to inform each category of individuals concerned about how their data will be processed (p. 7-8).

6. Ensure when responding to right of access requests that personal information of other parties is not revealed (p. 8-9).

7. Assess the appropriate competence of the recipient (internal or external) and then limit the transfer of personal information only when necessary for the legitimate performance of tasks covered by the competence of the recipient (p. 9).

8. Define proportionate conservation periods for the personal information processed within the scope of the whistleblowing procedure depending on the outcome of each case (p. 9-10).

9. Implement both organisational and technical security measures based on a risk assessment analysis of the whistleblowing procedure in order to guarantee a lawful and secure processing of personal information (p. 10-11).

TABLE OF CONTENTS

1. INTRODUCTION

1 Whistleblowing procedures are intended to provide safe channels for anyone who becomes aware and reports potential fraud, corruption, or other serious wrongdoings and irregularities. Whistleblowers believe that they are acting in the public interest when reporting an activity observed that is of a serious nature.

2 The Staff Regulations "SR" as well as the Conditions of Employment of Other Servants "CEOS"[1] contain an obligation for staff members and other persons working for the EU institutions and bodies ("EU institutions") to report in writing any reasonable suspicion of illegal activities to the hierarchy or to the European Anti-Fraud Office ("OLAF") directly. Some EU institutions have also adopted internal rules about whistleblowing by their staff members. As the whistleblowing arrangements serves as a detection mechanism to bring cases to the attention of OLAF, the duty to report concerns only serious wrongdoings and irregularities. The scope of these Guidelines is limited to the initial stage when EU institutions receive a report and not when it has been referred or sent directly to OLAF.

3 Whistleblowing procedures contain the processing of sensitive personal information. EU institutions are required to manage whistleblowing reports and ensure the protection of the personal information of the whistleblowers, the alleged wrongdoers, the witnesses and the other persons appearing in the report. These Guidelines explain and give hypothetical examples on how to apply the data protection principles in this specific context, which may affect individuals' private lives. The Guidelines also show that the data protection principles can be used to strengthen the whistleblowing procedures. The application of data protection principles will, inter alia, help creating reliable channels by reinforcing security aspects of the procedure.

4 External parties that enter into a contract with the EU institutions or contact the EU institutions (such as consultants, contractors, researchers etc.) should be informed that it is possible to report suspected fraud, corruption or other serious wrongdoings and irregularities.

5 This processing operation is likely to present specific risks[2] and therefore is subject to prior checking by the European Data Protection Supervisor ("EDPS").

2. SAFE CHANNELS FOR REPORTING FRAUD - ENSURE CONFIDENTIALITY

6 The most effective way to encourage staff to report concerns are to ensure them that their identity will be protected. Therefore, clearly defined channels for internal and external reporting and the protection of the information received should be in place. The identity of the whistleblower who report serious wrongdoings or irregularities in good faith should be treated with the utmost confidentiality as they should be protected against any retaliation. Their identity should never be revealed except in certain exceptional circumstances if the whistleblower authorises such a disclosure, if this is required by any

[1] The general legal framework for the EU staff acting as whistleblowers is set out in the Articles 22 a, 22b and 22c of the staff regulation, which according to Article 11 of Conditions of Employment of Other Civil servants of the EU apply by analogy to servants engaged under contract.
[2] Article 27(2)(a) and (b) of Regulation (EC) No 45/2001 (the 'Regulation').

subsequent criminal law proceedings, or if the whistleblower maliciously makes a false statement. In the latter case, these personal data can only be disclosed to judicial authorities.[3] A statement is maliciously made if the whistleblower report activities that he/she knows are not true. If an EU institution becomes aware of the fact that a whistleblower knew that the allegation made by him/her was unsubstantiated, the responsibility lies on the institution to prove the maliciousness of the allegations.

7 The person against whom an allegation has been made should be protected in the same manner as the whistleblower, since there is a risk of stigmatisation and victimisation within their organisation. They will be exposed to such risks even before they are aware that they have been incriminated and the alleged facts have been analysed to determine whether or not they can be substained.

8 Therefore, internal access to the information processed as part of the investigation of the allegations must be granted strictly on a need to know basis, that is, subject to the necessity to have access. Persons in charge of the management of reports could for example be subject to a reinforced obligation of secrecy. Personal information must also be stored securely (see security measures below).

9 Any whistleblowing- related personal information retained for statistical purposes should be made anonymous. EU institutions (especially smaller ones) should be particularly cautious with any information that may result in *indirect* identification. For instance, retaining both the type of whistleblowing cases together with the nationality of the whistleblower could lead to indirect identification and should therefore be avoided.

Example 1: *An EU Agency has explicit recommendations to its staff on how to guarantee the confidentiality of whistleblowers and the alleged wrongdoers during the initial assessment of a case. The EDPS stresses that the vulnerability of the involved parties is the same regardless of whether the case is ongoing or closed. The protection of whistleblowers and the alleged wrongdoers should therefore be considered also after the closure of a case.*

3. AVOID ABUSE OF THE PROCEDURE - SPECIFY THE PURPOSE

10 The scope of the procedure must be limited in order to avoid abuse of the procedure. The purpose of the whistleblowing procedure must be **clearly specified**[4] in the internal rules/policy of EU institutions. Internal rules or a policy should explicitly describe in which circumstances whistleblowing channels must be used and in which circumstances they should not. In general whistleblowing channels **should not be used** when staff may wish to exercise their statutory rights i.e. by lodging a request or complaint to the appointing authority under Art 90 of the SR or for harassment claims and personal disagreements when staff may address themselves to the HR, Mediation Service, confidential counsellor, or lodge a request for assistance under Art. 24 of the SR.

11 The internal rules or a policy should furthermore describe that sensitive information, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-

[3] See the EDPS case 2010-0458.
[4] Article 4(1)(b) of the Regulation.

union membership, and data concerning health or sex life[5] not relevant for the case should be avoided. This will help avoiding the collection of excessive data personal information (see below).

12 In principle, **whistleblowing should not be anonymous**. Whistleblowers should be invited to identify themselves not only to avoid abuse of the procedure but also to allow their effective protection against any retaliation. This will also allow a better management of the file if further information would be necessary.

4. AVOID PROCESSING EXCESSIVE PERSONAL INFORMATION

13 EU institutions may sometimes come into possession of personal information, which is clearly of no interest or relevance to the allegations. **Any such information should not be further processed**. This is particularly important for special categories of information. All investigators should be made aware of this rule.

Example 2: *A whistleblower reports that a colleague has committed a fraudulent activity. Within his statement, the whistleblower happens to disclose information about his colleague's health situation. It is clear to the institution that this information is completely irrelevant to the reported wrongdoing, and therefore it should not be further processed or returned to the sender.*

14 A good practice is to implement a general recommendation, for example in the internal rules of procedure, to the persons handling the files reminding them of the rules of data quality[6] and recommend them to ensure the respect of the rules.

5. IDENTIFY WHAT PERSONAL INFORMATION MEANS IN THIS CONTEXT

15 Personal information is defined as any information that relates to an identified or identifiable natural person.[7] Personal information does not only include information about an individual's private life and family life, but also information regarding an individual's activities, such as his or her working relations and economic or social behaviour[8]. This needs to be considered, for instance, when determining the scope of the data subject's right of access. In most cases, personal information includes identification data (contact details e.g.) but also information that relates to the behaviour of an individual.

Example 3: *The report of the whistleblower includes information that identifies the alleged wrongdoer and witnesses. The report itself is also personal information of the whistleblower since it relates to his or her behaviour (as a whistleblower).*

[5] Article 10(1) of the Regulation.
[6] Article 4(1) of the Regulation.
[7] Article 2(a) of the Regulation.
[8] Article 29 Working Party Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20 June 2007.

16 The same piece of information may relate to different individuals at the same time. The whistleblower report may contain personal information of witnesses and third parties (persons merely quoted in the file), the persons against whom the allegations have been made and the whistleblower himself.

17 On the other hand, the mere fact that a name is mentioned in a document does not necessarily make all the information contained in that document "data relating to that person". In many situations, information can be considered to relate to an individual only when it's about that individual.

Example 4: *An EU institution might produce a report considering whether to refer the case to OLAF or not. The analysis may refer to the whistleblower as a source but the whole report is not personal information relating to the whistleblower.*

6. INFORM EACH CATEGORY OF INDIVIDUALS

18 Information on whistleblowing procedures should be provided to the individuals in a very prominent way, which will require a **two-step** procedure. While placing a data protection statement on the website (or within a public or internal-facing document) is certainly a positive step, the EDPS considers that this is **not sufficient**, as the information could be overlooked. All individuals affected by a particular whistleblowing procedure should also be directly provided with a specific data protection statement as soon as practically possible, for example by email. Affected individuals will usually include whistleblowers, witnesses, third parties (members of staff or others that are merely quoted) and the person(s) against whom the allegations has been made.

6.1. Information to the whistleblower (Article 11 of the Regulation)

19 In this context, it is important to inform about possible recipients or categories of recipients[9] of the whistleblower's personal information. In addition, the data protection statement should also inform the persons about the consequences of abusive use (if the whistleblower maliciously makes a false statement) of the whistleblowing procedure, for instance disciplinary measures.

6.2. Information to the alleged wrongdoer (Article 12 of the Regulation)

20 In certain cases, informing the person against whom an allegation has been made at an early stage may be detrimental to the case. In these cases, provision of specific information might need to be deferred.[10] Deferral of information should be decided on a case by case basis. The reasons for any restrictions should be documented, and made available to the EDPS if requested in the context of a supervision and enforcement action. These reasons should prove, for instance, that there is a high risk that giving access would hamper the procedure or undermine the rights and freedom of the others. The reasons should be documented before the decision to apply any restriction or deferral is taken.

[9] Article 11(1)(c) of the Regulation.
[10] Article 20 of the Regulation.

6.3. Information to witnesses (Article 11 of the Regulation)

21 Specific information to witnesses should be provided as soon as practically possible, for instance before they are being interviewed by the institution.

6.4. Information to third parties (Article 12 of the Regulation)

22 Depending on the case, informing all the third parties mentioned in a whistleblowing report might involve a disproportionate effort.[11] The assessment whether it is disproportionate or not to inform third parties must be carried out on a case-by-case basis. Moreover, in certain cases, informing individuals would be an additional processing operation that could be more intrusive than the initial one.

Example 5:
a) A whistleblower attaches to the report a list of the clients (200 people) of a hotel to prove that the alleged wrongdoer was in the hotel at a certain date. The 199 other clients have no link with the case and their information are not processed further by the institution. They should not be informed.
b) A whistleblower provides together with the report an USB key containing exchanges of emails with the alleged wrongdoer and a few other staff members. The institution conducts a preliminary analysis and processes the information of the other staff members. The members of staff concerned should be informed.

7. ASSESS THE INDIVIDUAL'S RIGHT OF ACCESS AND LIMITATIONS

23 When considering access rights, institutions should consider the status of the requester and the current stage[12] of the investigation. The level and sensitivity of information held (and any associated risks in disclosure) will vary depending on whether the request is made by:

- the person against whom an allegation has been made
- the whistleblower
- a witness
- third parties

24 Institutions must carry out a case-by-case assessment of each individual case and document the reasons underlying their decision. This should take into account the type of information held and whether any exceptions of the Regulation are applicable.

25 **When access is granted to the personal information of any concerned individual, the personal information of third parties such as informants, whistleblowers or witnesses should be removed from the documents except in exceptional circumstances** if the whistleblower authorises such a disclosure, if this is required by any subsequent criminal law proceedings or if the whistleblower maliciously makes a

[11] Article 12(2) of the Regulation.
[12] Article 20(1)(a) of the Regulation.

false statement. If a risk remains of third party identification, access should be deferred. The Article 29 Working Party recommended that: *"Under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower …except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed"*.[13] This is especially important to guarantee that individuals are protected from any potential risks involved in disclosing their personal information.

Example 6: *An EU employee accused of serious wrongdoings asks the institution for all personal information held on him in relation to the accusations. Much of this information is included in testimonies given by the whistleblower. Even if the whistleblowers name is deleted from these documents, their identity would be obvious through reference to the specific events, situations and contexts described. Thus, the institution should defer release of this information with regard to the protection of the data subject or of the rights and freedoms of others (Article 20(1)(c)).*

8. LIMIT TRANSFERS

26 Different obligations apply depending on whether the recipients are an EU institution (in this context when an institution transfers data to OLAF), or someone subject to Directive 95/46 (such as a national court or other types of recipients).[14] **The requirements for transferring data must be assessed on a case-by-case basis**. In particular, personal information should be transferred only when necessary for the legitimate performance of tasks covered by the competence of the recipient.

9. DEFINE CONSERVATION PERIODS DEPENDING ON THE OUTCOME OF THE CASE

27 Personal information must not be kept for a longer period than necessary having regard to the purpose of the processing.[15] Therefore, different conservation periods should apply depending on the information in the report and how the case is dealt with.

28 Firstly, as mentioned above, personal information that is not relevant to the allegations should not be further processed (see paragraph 4).

29 Secondly, when an initial assessment is carried out but it is clear that the case should not be referred to OLAF or is not within the scope of the whistleblowing procedure the report should be deleted as soon as possible (or referred to the right channel if it for example concerns alleged harassment). In any case, personal information should be deleted promptly and usually within two months of completion of the preliminary assessment[16], since it would be excessive to retain such sensitive information.

[13] Article 29 Working Party Opinion on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, adopted on 1 February 2006, pg. 14
[14] Articles 7, 8 and 9 of the Regulation.
[15] Article 4(1)(e) of the Regulation.
[16] Article 29 Working Party Opinion 1/2006, WP 117, pg. 12.

30 Thirdly, if it is clear after the initial assessment that a report should be transferred to OLAF the EU institution should carefully follow what actions OLAF takes. If OLAF starts an investigation it is not necessary for the EU institutions to keep the information for a longer period. In case OLAF decides not to start an investigation, the information should be deleted without delay.

31 In case a longer retention period is envisaged, access to the personal information should still be limited (see security measures below). It is a good practice to separate these reports from the main case management system/daily system in use.

Example 7: *An EU institution has received several whistleblowing reports through the whistleblowing channel. One report concerns alleged harassment and is therefore directly referred to the unit dealing with these cases. Two other reports are likely to concern fraud and therefore transferred to OLAF which starts an investigation in one of the cases. The institution applies a conservation period of 5 years on the report where OLAF does not start an investigation. In this situation the EDPS consider that a period of 5 years is excessive and the report should be deleted as soon as possible.*

10. IMPLEMENT ADEQUATE SECURITY MEASURES

32 The controller should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal information to be processed.[17] This is not only a clear legal requirement, as previously mentioned the confidentiality regarding all the procedure is of the utmost importance to encourage staff to report any concerns they may have. Furthermore, security measures need to reflect the sensitive nature of the personal information being processed. In this context it is essential to put in place appropriate security measures in order to effectively prevent personal information from being accessed by non-authorised persons and to guarantee its integrity.

33 **The need for these security measures has to be analysed in light of the risks regarding the whistleblowing procedure** whatever it is a manual or an automatic one: **an information security risk assessment**. Once the risks to the personal information involved are determined a subsequent analysis can be performed to determine which measures to implement taking into account, also, the cost of these security measures and their viability. As risks evolve over time, it is necessary for the EU institution to review its analysis, the selection of security measures and their effectiveness regularly.

34 Detailed advice on information on information security risk management can be found in the EDPS '[Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001]'.

[17] See Article 22 of the Regulation.

Example 8: *Of special relevance for whistleblowing files:*
a) Staff that can have access to the personal information must be strictly limited on a need to know-basis. Staff with access must be subject to reinforced obligation of secrecy and access to the whistleblowing reports must be monitored whatever in electronic or paper form.
b) From a technical point of view, the common requirements of access control needs to be fully implemented: effectively limit and control who has access to whistleblowing cases, log accesses and review regularly both the accesses and the access rights.
c) Encryption needs to be specially considered due to the high needs of confidentiality of this information. Notwithstanding the use of encryption, safeguard mechanisms need to be implemented to allow the access to the information when needed (keys shared, record and safe keeping of passwords...).

11. BE ACCOUNTABLE!

35 Accountability means that organisations must respect their data protection obligations and **be able to demonstrate that they do so**.

36 Accountability is not specific to personal information within a whistleblowing procedure, but applies to all operations that process personal information.

37 Any organisation that collects, uses and stores (collectively known as processing) personal information is responsible and accountable for complying with data protection rules.

38 In general, institutions must be transparent and explicit about how they process the personal information related to whistleblowing procedures. They must document their policies and make users aware of them. The right to privacy also exists in the workplace and people must be made aware of the procedure. Institutions cannot assume that staff will know.

39 The best way for an institution to be accountable is for it to consider the data protection implications of new processes at the design stage (**data protection by design**). Different processing operations and different technologies require different safeguards. By involving their data protection officer (DPO) early in the process, he or she will be able to offer valuable advice and guidance.

40 The questions listed below outline the main issues to consider:

a. **Confidentiality:** How do you protect the persons involved?
b. **Specify the purpose:** When to use the whistleblowing channel?
c. **Avoid excessive information:** What information is necessary for the allegations made?
d. **Identify the meaning of personal information:** What is personal information in this specific report?
e. **Inform each category of individuals:** Who are affected by this specific report?
f. **Different conservation periods should apply:** How long do I need to keep the report?

g. **Conduct an information security risk assessment:** What are the risks your whistleblowing cases may suffer and how are you going to protect yourself from them?

41 To demonstrate accountability also implies documentation of the procedure and its implementation. The following should be documented:

a. a **policy or internal rules or decision** on whistleblowing;

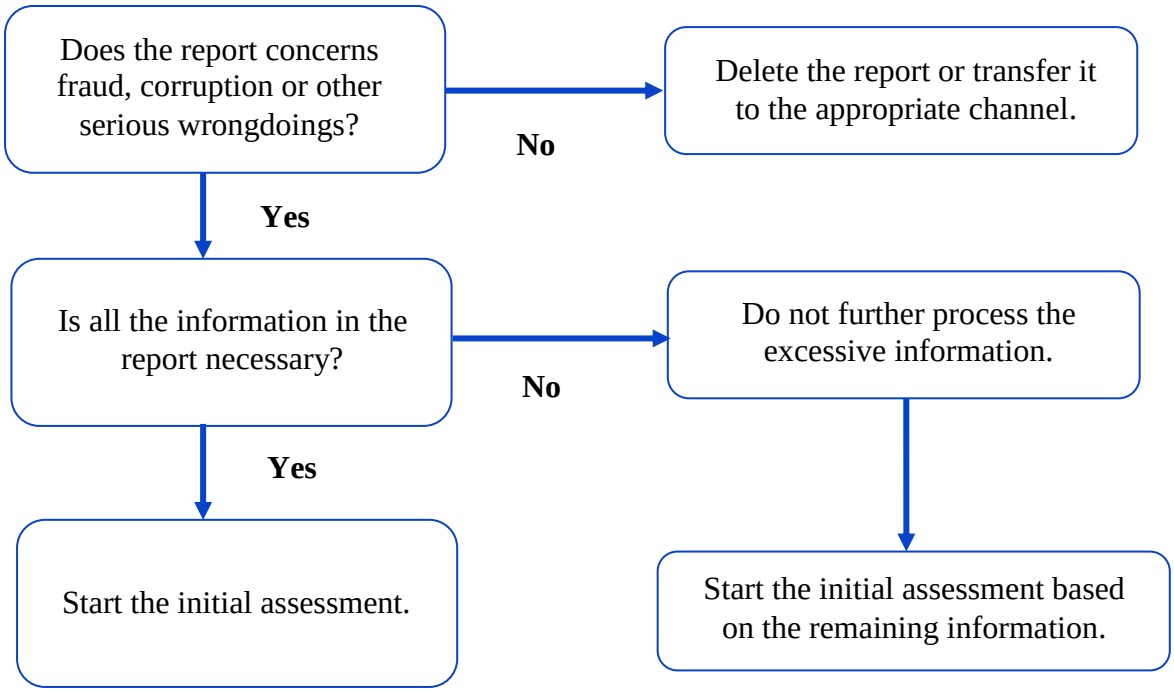
b. **limitations to the right of access should** be documented, not only on which grounds it is based but also the reasoning why it applies to this specific situation;

c. any **deferral of information** to the individual;

d. the **risk assessment** conducted for this specific procedure.

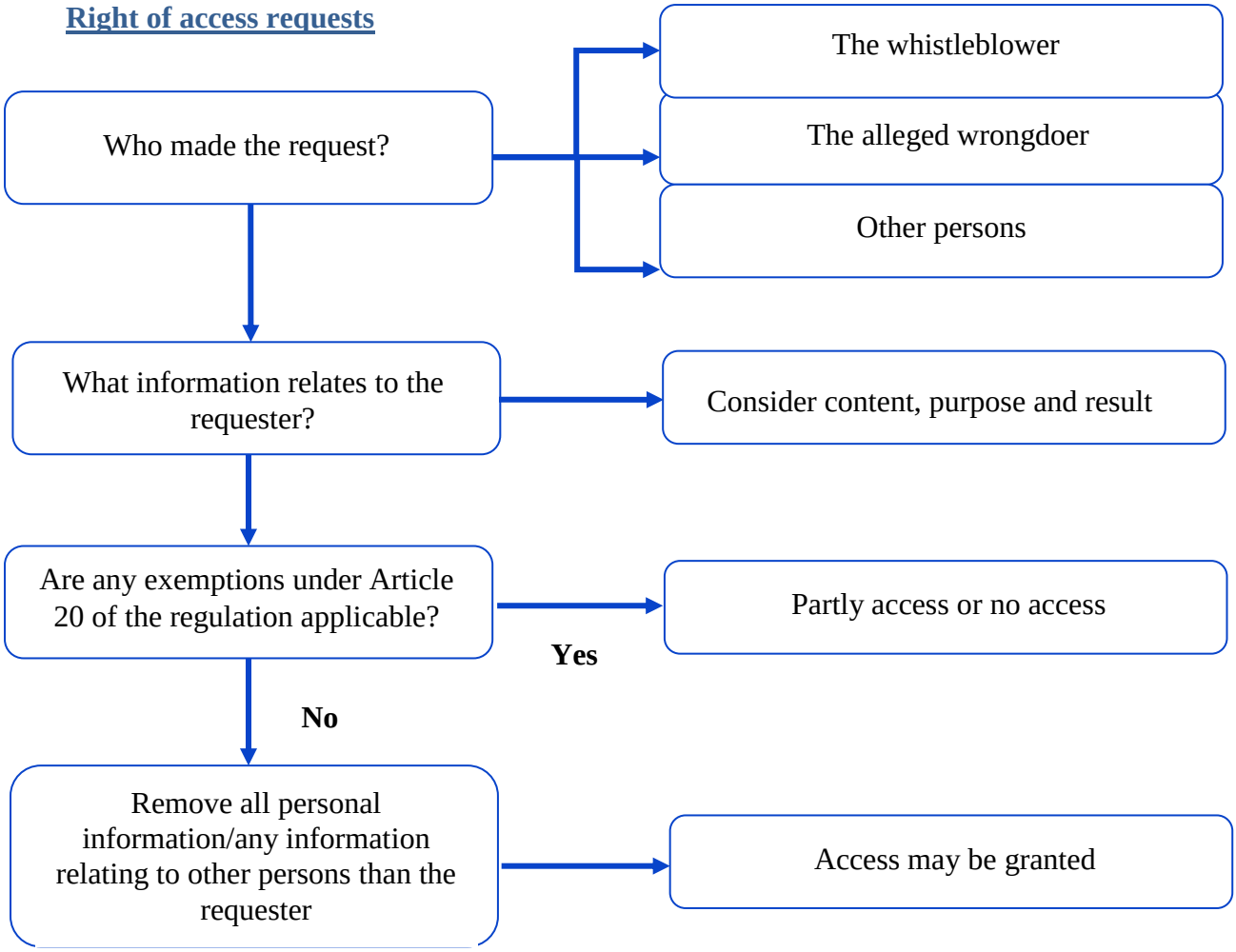
12. FLOWCHARTS WHISTLEBLOWING PROCEDURES

12.1. Handling whistleblowing reports

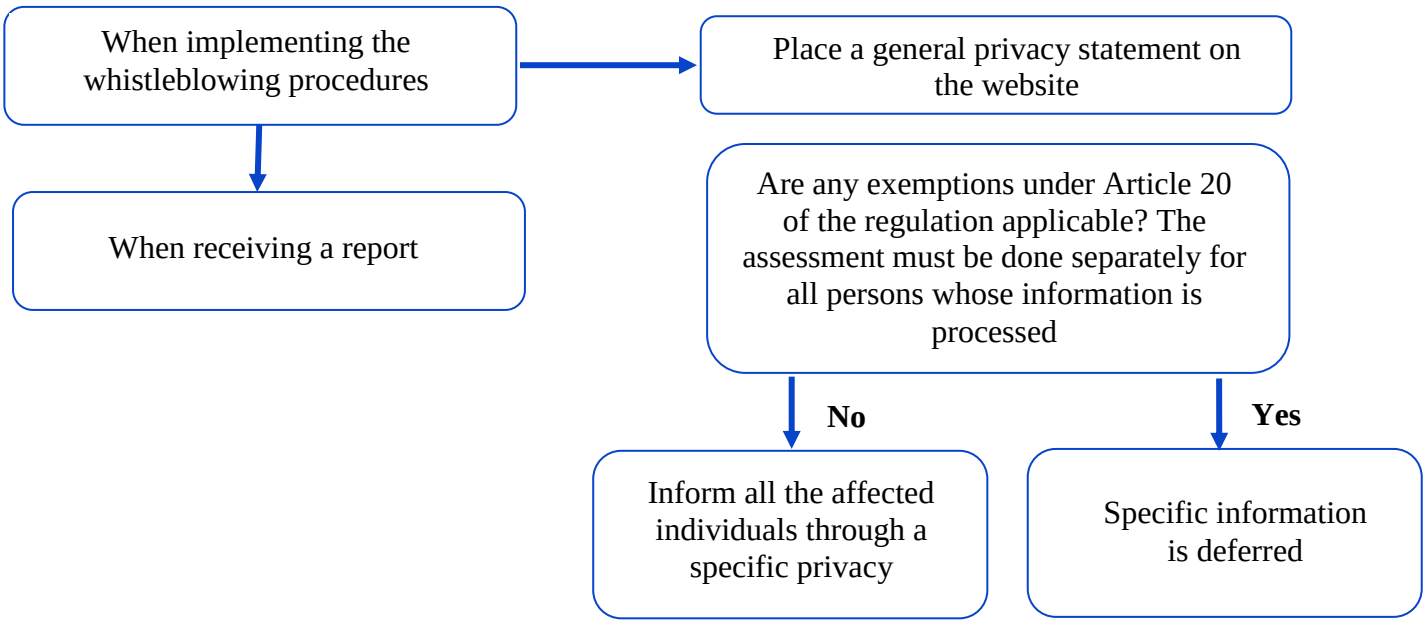


12.2. Ensuring individuals' rights

Right of access requests



How to inform the individuals properly



FURTHER READING

Examples of EDPS Opinions

2014-0828 - Opinion on the European Ombudsman's Whistleblowing Procedure

2015-0061 - Opinion on the European Research Council Executive Agency's procedure on handling internally and reporting potential fraud and irregularities

2015-0349 - Opinion on the whistleblowing procedure of the General Secretariat of the Council of the European Union

2015-0569 - Opinion on the whistleblowing procedure of the European Fisheries Control Agency

Other documents

Protection of whistleblowers - recommendation CM/Rec(2014)7 and explanatory memorandum - Council of Europe

Whistleblowing in Europe, legal protection for whistleblowers in the EU - Transparency National International principles for whistleblower legislation - Transparency National