EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on processing personal information within a whistleblowing procedure

December 2019

Executive Summary

Whistleblowing serves to disclose wrongdoing or corruption. A key challenge to prevent corruption is to detect and expose bribery, fraud, theft, and other acts of wrongdoing in the work place. Whistleblowing reveals such unethical behaviour.

Since whistleblowers can face retaliation in the form of harassment, firing, blacklisting, threats and/or have their disclosures ignored, the law protects whistleblowers from being retaliated against. Confidentiality, including protection of identity, is therefore an essential and effective way to encourage staff to report concerns.

These guidelines provide practical guidance to the EU institutions, bodies and agencies both before and after the implementation of a whistleblowing procedure to ensure that they comply with the data protection obligations as set out in Regulation (EU) 2018/1725.

These guidelines are an update of the guidance on whistleblowing published in July 2016.

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. 5).

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

3. Apply the principle of data minimisation: only process personal information, which is adequate, relevant and necessary, for the particular case (p. 6-7).

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, bodies and agencies have internal rules in place and are able to provide documented reasons before taking such a decision (p. 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. 9-10).

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. 10).

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. 10-11).

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. 11-12).

TABLE OF CONTENTS

1. INTRODUCTION

1 Whistleblowing procedures are intended to provide safe channels for anyone who becomes aware of and reports potential fraud, corruption, or other serious wrongdoing and irregularities. Whistleblowing procedures protect whistleblowers and disclosures that are in the public interest. Whistleblowing procedures are not intended for the reporting of a grievance or making a complaint.

2 These guidelines are intended to provide practical advice and instructions to the EU institutions, bodies and agencies (EUIs) on the processing of personal data within a whistleblowing procedure, to ensure that they comply with their data protection obligations as set out in Regulation (EU) 2018/1725[1] (the Regulation).

3 The EDPS has developed these guidelines based on long-term experience. A first edition was published in July 2016; in the meantime, new data protection rules applicable to the EUIs have replaced Regulation (EC) 45/2001. The new Regulation mirrors the General Data Protection Regulation (GDPR) applicable to organisations in the EU/EEA. In addition, a new Directive on the protection of persons who report breaches of EU law[2] (the Directive) has been agreed[3]. These Guidelines have been updated to reflect the current Regulation as well as some elements of this Directive even though it is not applicable to EUIs.

4 The Staff Regulations (SR) as well as the Conditions of Employment of Other Servants (CEOS)[4] contain specific obligations for staff members and other persons working for the EUIs to report in writing any reasonable suspicion of illegal activities to the hierarchy or to the European Anti-Fraud Office (OLAF) directly. EUIs have also adopted internal rules about whistleblowing by their staff members. As the whistleblowing arrangements serve 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 EUIs receive a report and not when it has been referred or sent directly to OLAF.

5 Whistleblowing procedures contain the processing of special categories of data. EUIs 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 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, therefore, help creating reliable channels by reinforcing the security aspects of the procedure.

[1] OJ L 295/39, 21/11/2018.
[2] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of persons who report breaches of Union law, 2018/0106 (COD).
[3] The legislation will now be formally signed and published in the Official journal.
[4] The general legal framework for the EU staff acting as whistleblowers is set out in the Articles 22a, 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.

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

2. SAFE CHANNELS FOR REPORTING FRAUD - ENSURE CONFIDENTIALITY

7 The most effective way to encourage staff to report concerns is to ensure 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 reports 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 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.[5] A statement is maliciously made if the whistleblower reports activities that they know is untrue. If an EUI becomes aware that a whistleblower made an unsubstantiated allegation, the responsibility lies on the institution to prove the maliciousness of the allegations.

8 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 sustained.

9 Whistleblowing reports may also include personal information about third persons, such as witnesses or colleagues. Their personal information should also be protected at all stages of the procedure.[6]

10 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, in other words, subject to necessity. Those 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).

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

[5] See the EDPS case 2010-0458.
[6] Recital 76 of the Directive.

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

12 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**[7] in the internal rules/policy of EUIs. 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 Article 90 of the SR or for harassment claims and personal disagreements when staff may address themselves to the HR, the mediation service, a confidential counsellor or lodge a request for assistance under Article 24 of the SR.

13 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-union membership, and data concerning health or sex life[8] not relevant for the case should not be collected file. This will help avoid the collection of excessive personal information (see section 4 below).

14 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 better management of the file if it is necessary to gather further information.

4. AVOID PROCESSING EXCESSIVE PERSONAL INFORMATION

15 EUIs 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 fraud. 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.*

[7] Article 4(1)(b) of the Regulation.
[8] Article 10(1) of the Regulation.

16 A good practice is to implement a general recommendation, for example in the internal rules of procedure, for those handling whistleblowing files to remind them to respect the rules on data quality.[9]Another good practice, as specified in the Directive[10], would be to provide data protection training to those members of staff who are responsible for handling requests.

5. IDENTIFY WHAT PERSONAL INFORMATION MEANS IN THIS CONTEXT

17 Personal information is defined as any information that relates to an identified or identifiable natural person.[11] Personal information not only includes 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[12]. This needs to be considered, for instance, when determining the scope of the individual's (data subject) right of access. In most cases, personal information includes identification data (for example, contact details) but also information that relates to the behaviour of that 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).*

18 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.

19 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

20 Information on whistleblowing procedures should be provided to the individuals in a very prominent way, which will involve a **two-step** procedure. While placing a data protection notice on the website (or within a public or internal-facing document) is encouraged, the EDPS **does not** consider this **sufficient**, as the information could be

[9] Article 4(1) of the Regulation.
[10] Recital 74 of the Directive.
[11] Article 3(1) of the Regulation.
[12] Article 29 Working Party Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20 June 2007.

overlooked. All individuals affected by a whistleblowing procedure should be directly provided with a specific data protection notice 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 15 of the Regulation)

21 In this context, it is important to inform all those implicated in the procedure who their personal information will be shared with (potential recipients or categories of recipients[13]). In addition, the data protection notice should also inform them about the consequences of the abuse of the whistleblowing procedure (if the whistleblower maliciously makes a false statement for instance), such as disciplinary measures.

6.2. Information to the alleged wrongdoer (Article 16 of the Regulation)

22 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 restricted.[14] EUIs must have internal rules in place to be able to restrict information (see paragraph 26 below). 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.

6.3. Information to witnesses (Article 15 of the Regulation)

23 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 16 of the Regulation)

24 Depending on the case, informing all the third parties mentioned in a whistleblowing report might involve a disproportionate effort.[15] The assessment of 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 original one.

[13] Article 15(1)(d) of the Regulation.
[14] Article 25 of the Regulation.
[15] Article 16(5)(b) of the Regulation.

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, a 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

25 When considering access rights, EUIs should consider the status of the requester and the stage[16] 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

26 EUIs should ensure that there is a clear legal basis before applying any restriction under Article 25 of the Regulation. This means that EUIs should have adopted internal rules covering the exceptional cases where information could be deferred. In addition, before applying a restriction in a specific case, a necessity and proportionality test must be carried out and EUIs must document the reasons underlying their decision in order to be accountable. For more information on internal rules and the assessment on a case-by-case basis, please see the EDPS Guidance on Article 25 of the new Regulation and internal rules. Furthermore, EUIs might need to distinguish between an internal justification on the use of the restriction and a general one to be communicated to the requester under Article 25(6), unless such information could be deferred under Article 25(8).

Example 6: *A whistleblower (A) reports suspected fraud by a colleague and superior (B). After the investigation is finished, B requests access to her personal data processed for this purpose. Parts of the allegations made by A qualify as personal data of B. The EUI might be able to justify a restriction under Article 25(1)(h) concerning the fact that A provided the data, and if it could be assumed that A provided this information, A might be subject to retaliation by B. This would need to be documented internally. Obviously, B should not be told that the reason for the restriction is that A could suffer retaliation since it would cancel the effect of the restriction in line with Article 25(8). Therefore, the information communicated to B under Article 25(6) would need to be formulated in a more general way.*

[16] Article 25(1)(b) and (f) of the Regulation.

27 **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[17] or if the whistleblower maliciously makes a false statement. If a risk remains of third party identification, access should be deferred. The Directive provides for a duty of confidentiality (Article 16(1)) with an obligation for Member States to ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members without the explicit consent of the person. This is especially important to guarantee that individuals are protected from any potential risks involved in disclosing their personal information.

Example 7: *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 25(1)(h)), provided that it is laid down in the internal rules of the EUI.*

8. LIMIT TRANSFERS

28 Different obligations apply depending on whether the recipients are EUIs (in this context when an institution transfers data to OLAF), or a recipient subject to the GDPR (such as a national court or others).[18] **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

29 Personal information must not be kept for a longer period than necessary with regard to the purpose of the processing.[19] Therefore, different conservation periods should apply depending on the information reported and how the case is dealt with:

30 Personal information that is not relevant to the allegations should not be further processed (see section 4) and deleted with undue delay.[20]

31 If following an initial assessment 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 for example it concerns alleged

[17] Article 16(2) of the Directive, *[...] the identity may however be disclosed only where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including the rights of defence of the person concerned.*
[18] Article 9 of the Regulation.
[19] Article 4(1)(e) of the Regulation.
[20] Article 17 of the Directive, last sentence.

harassment). In any case, personal information should be deleted promptly and usually within two months of completion of the preliminary assessment[21], since it would be excessive to retain such sensitive information.

32 If it is clear after the initial assessment that a report should be transferred to OLAF the EUI should carefully monitor what actions OLAF takes. If OLAF starts an investigation, it is not necessary for the EUI to keep the information for a longer period. In case OLAF decides not to start an investigation, the information should be deleted without delay.

33 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 8: *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 case that OLAF does not investigate. In this situation the EDPS considers that a period of 5 years is excessive and that the report should be deleted as soon as possible.*

10. IMPLEMENT ADEQUATE SECURITY MEASURES

34 The EUI (or data controller i.e. the entity who determines the purposes and means of the processing of personal data) should implement the 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.[22] Confidentiality is a clear legal requirement and is an important element in encouraging 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.

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

36 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 (to be updated).

[21] Article 29 Working Party Opinion 1/2006, WP 117, pg. 12.
[22] Article 33 of the Regulation.

Example 9: *Of special relevance for whistleblowing files:*
a) Staff permitted to have access to the personal information must be strictly limited on a need to know-basis. Staff with access must be subject to a reinforced obligation of secrecy and access to the whistleblowing reports must be monitored whether in electronic or paper form.
b) From a technical point of view, the requirements of access control needs to be fully implemented by: effectively limiting and controlling who has access to whistleblowing cases, accessing logs and regularly reviewing both access to the logs 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 access to the information when needed (shared keys, recording and safe keeping of passwords...).

11. BE ACCOUNTABLE!

37 Accountability means that EUIs must respect their data protection obligations and **be able to demonstrate that they do so.** (Articles 4(2) and 26 of the Regulation)

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

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

40 In general, EUIs 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 and data protection also exists in the workplace and people must be made aware of the procedure. EUIs cannot assume that staff will know. (Article 14 of the Regulation)

41 The best way for an EUI to be accountable is for it to consider the data protection implications of new processes at the design stage (**data protection by design**, Article 27 of the Regulation). Different processing operations and different technologies require different safeguards. By involving their data protection officer (DPO) early in the process, they will be able to offer valuable advice and guidance.

42 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 needed in the context of 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 is affected by the whistleblowing?

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 potential security risks to the personal information contained in whistleblowing cases and how are you going to mitigate those risks?

43 To demonstrate accountability, the procedure and its implementation must be documented. The following documents are required:

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

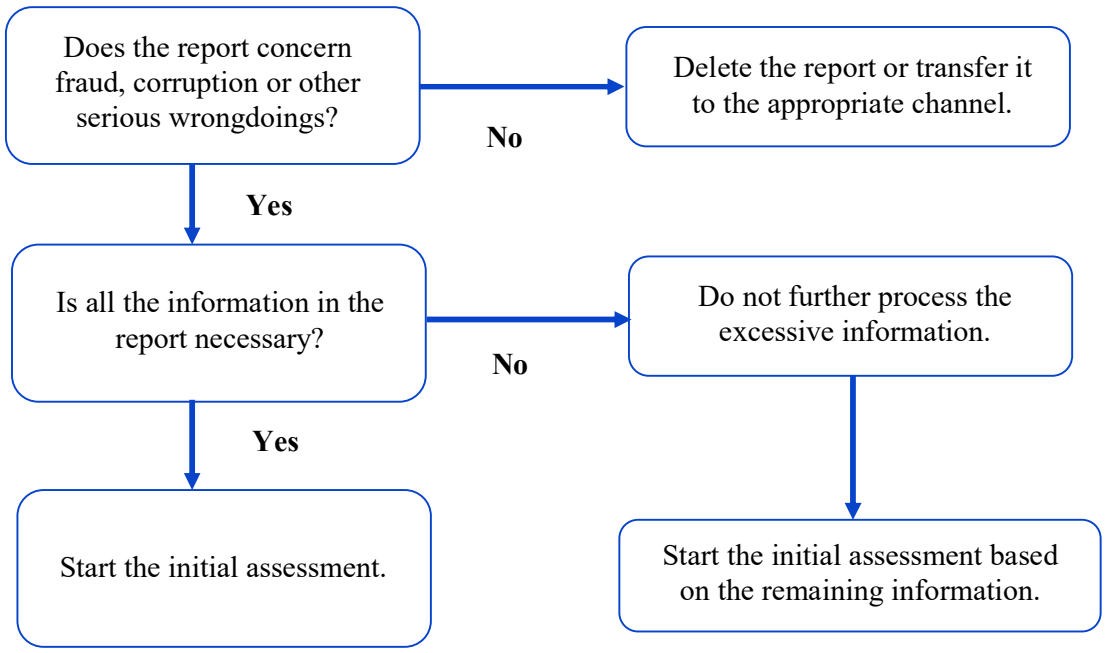
b. **limitations to certain rights of data subjects** (included in EUIs internal rules), the grounds on which the limitations are based and the reasoning for the applications of such restrictions

c. any **deferral of information** to the individual (in line with the internal rules);

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

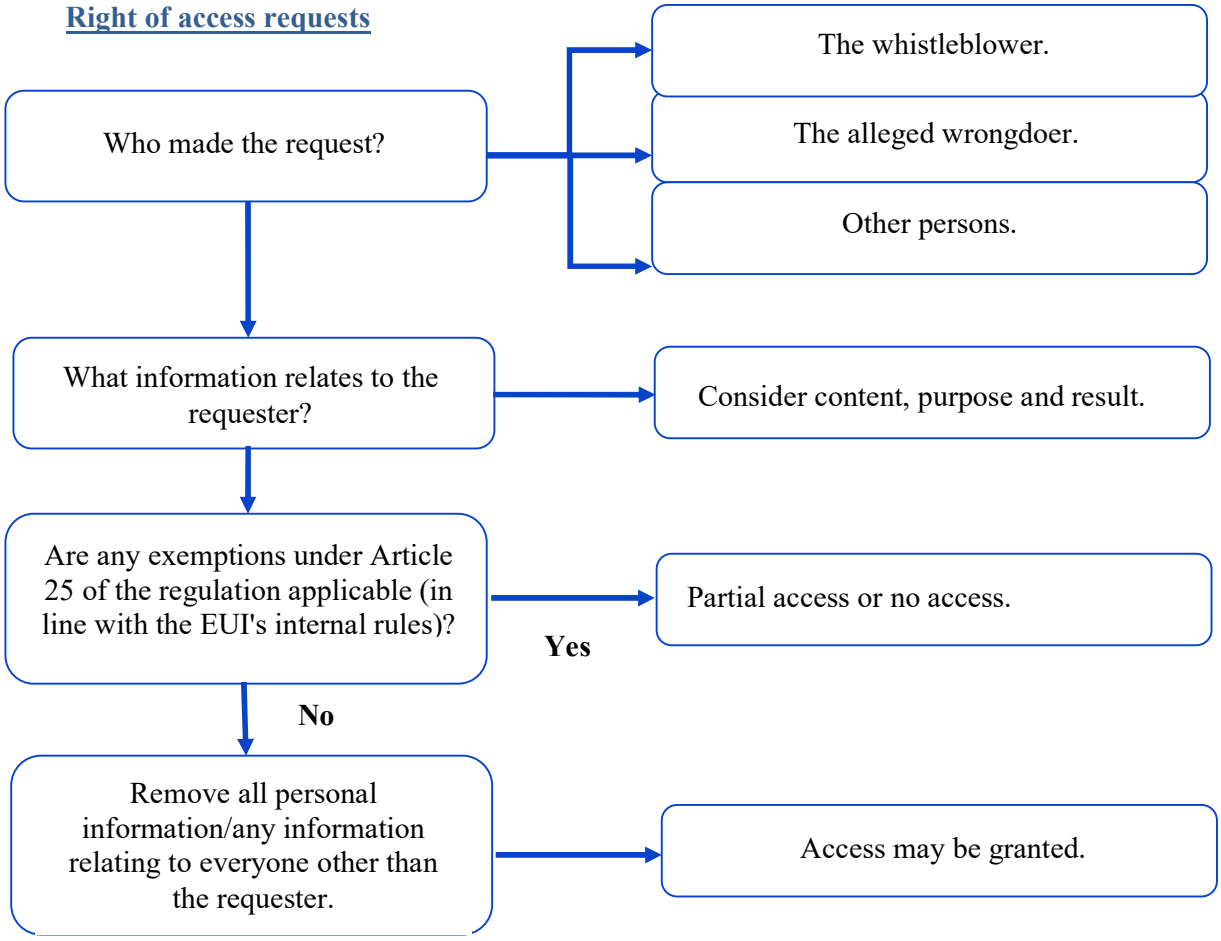
12. FLOWCHARTS WHISTLEBLOWING PROCEDURES

12.1. Handling whistleblowing reports

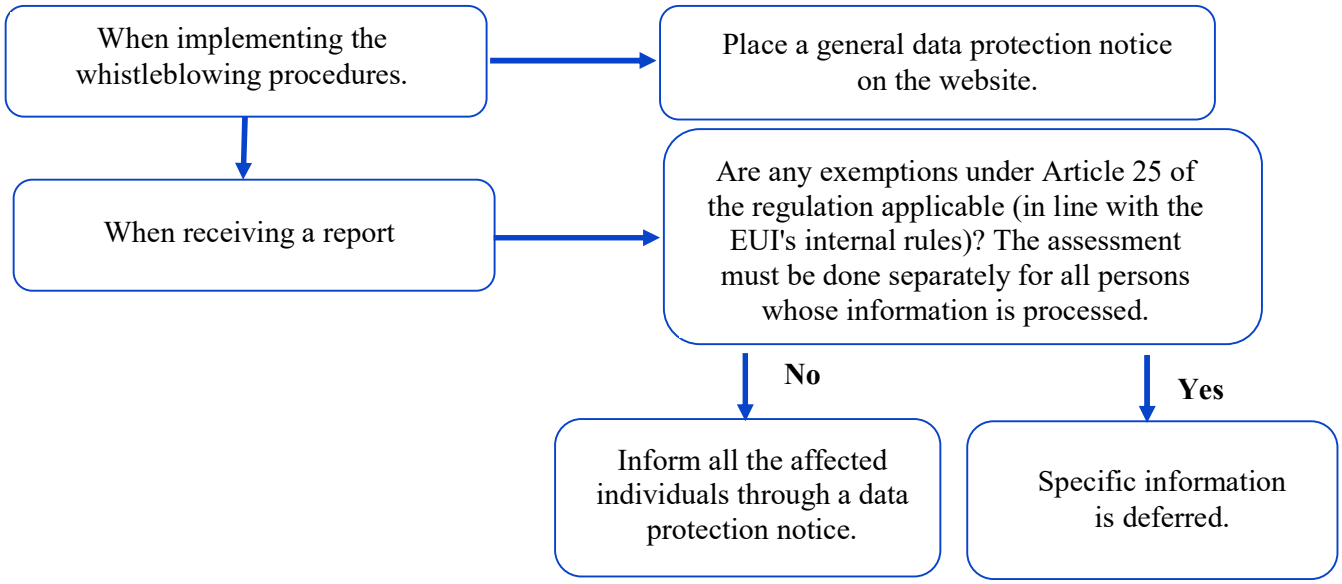


12.2. Ensuring individuals' rights

Right of access requests



How to inform the individuals properly



FURTHER READING

The Directive on the protection of persons who reports breaches of Union law

Examples of EDPS Opinions

2016-1083 - Opinion on EMCDDA's internal procedures and guidelines on whistleblowing

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

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