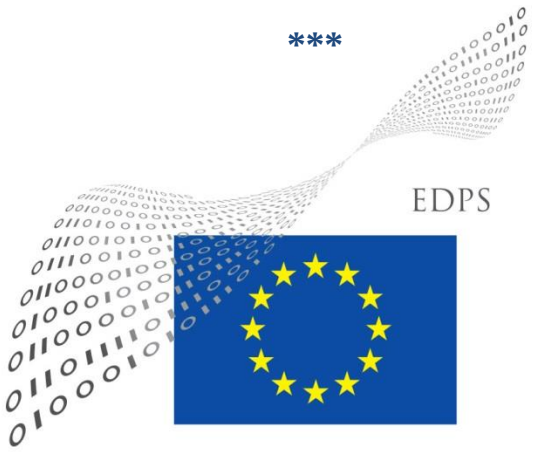
EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on processing personal information in administrative inquiries and disciplinary proceedings

***



18 November 2016

EXECUTIVE SUMMARY

If a staff member has allegedly acted in bad faith either intentionally or through negligence, they may be confronted with a potential breach of the Staff Regulations. The EU institution may launch an administrative inquiry or a disciplinary proceeding in order to verify whether there has been serious misconduct, fraud or any other irregularity affecting the financial or other interests of the EU.

It is of paramount importance that written rules and data protection safeguards are adopted before an inquiry is launched in the best interests of both the EU institution and the individuals involved. On the basis of a documented assessment, investigators should choose the least intrusive means to collect data in light of the necessity and proportionality principles. The person under investigation and all individuals involved in an inquiry should be aware of their main data protection rights and how to exercise them in this context.

These Guidelines are designed to help EU institutions and their investigators prepare and implement their procedures in administrative inquiries or disciplinary proceedings, so that the processing of personal data (or personal information) is lawful, fair and transparent in compliance with their obligations set out in the data protection Regulation (EC) 45/2001.

List of recommendations:

R1: Adopt a specific legal instrument, to set out specific rules about the processing operation in an administrative inquiry.

R2 : Ensure that the data protection rules on the use of different means for collecting potential evidence for the investigation are reflected in a Manual including specific guidance, which could be included in the specific legal instrument; the least intrusive means are used for the collection of personal information.

R3: Investigators should be fully aware of the restrictive rules, which apply to the processing of sensitive information. The principle of data minimisation should be applied: only personal data, which are adequate, relevant and necessary, should be collected to the purpose of the particular case and they should not be further processed without specific authorisation.

R4: 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 your institution is able to provide documented reasons before taking such a decision.

R5: Adopt proportionate retention periods for the personal information kept in the inquiry and in the disciplinary files depending on the outcome of each case.

R6: Assess the appropriate competence of the recipient (internal or external) and then limit the transfer of personal information to only what is strictly relevant and necessary.

R7: If an external investigator is necessary, their data protection obligations should be specified in a contract with your institution.

R8: Implement both organisational and technical security measures based on a risk assessment analysis in order to guarantee a lawful and secure processing of personal information.

TABLE OF CONTENTS

1. INTRODUCTION

1. These Guidelines are based on the EDPS' supervisory experience in the field of administrative inquiries and disciplinary proceedings. Our fruitful exchange with the DPO network has helped guide us on with the practical aspects of an administrative inquiry in their own institutions[1]. Our consultations with IDOC, the Data Protection Officer of ECB and the Data Protection Officer of CHAFEA were also very useful.

2. These procedures concern primarily staff of the EU institutions and bodies. An inquiry may be launched for instance in the case of a psychological or sexual harassment, if a staff member carries out external activities without permission during office hours, a conflict of interest situation or a suspicion of a staff member inflating the working hours on his timesheets. Affected individuals, apart from the alleged victim and the person under investigation, might also include witnesses and third parties (persons merely quoted in the file). If, following the administrative inquiry, there is enough evidence that the person under investigation has committed a serious misconduct, a fraud or any other irregularity affecting the financial or other interests of the public administration, a disciplinary proceeding can be initiated. The severity of the disciplinary sanction will depend on the seriousness of the misconduct. The accused person can be dismissed or be suspended for a specific period.

3. Most EU institutions[2] carry out their own inquiries and disciplinary proceedings. The Investigation and Disciplinary Office of the Commission (IDOC) is the body responsible for conducting administrative inquiries and disciplinary proceedings on behalf of the European Commission[3] and among other EU institutions[4].

4. The aim of these Guidelines is to provide guidance to all EU institutions to set out specific data protection safeguards in light of Regulation (EC) 45/2001 (the Regulation) before and during an inquiry and a disciplinary proceeding, as well as after the conclusion of the procedure. These safeguards reflect both the EU institutions' obligations and the individuals' rights. They will ensure that an inquiry and a disciplinary proceeding are carried out in a lawful, fair, proportionate and secure way, in the best interests of both the EU institution and the affected individuals.

5. Administrative inquiries and disciplinary proceedings entail the processing of sensitive personal information. Such processing is likely to present specific risks[5] to the rights and freedoms of the individuals implicated in the proceedings and they should be

[1] 38th DPO meeting hosted by ENISA, in Athens, on 5 November 2016.
[2] "EU institution" refers to every institution, body and agency of the EU.
[3] IDOC acts as a co-controller with the different DGs of the Commission.
[4] IDOC acts a processor with the decentralised agencies on the basis of the SLA concluded between them. In particular, IDOC acts as a help-desk in individual cases, providing them with procedural advice, models and templates for documenting the various procedures. In order to provide further assistance, IDOC has already organised training about the conduct of administrative inquiries and disciplinary procedures for the decentralised agencies. IDOC is further working on a model decision for administrative inquiries and disciplinary procedures for these agencies. IDOC intends to provide trainings to EU institutions upon request.
[5] Article 27(2)(a) and (b) of the Regulation.

therefore subject to prior checking by the EDPS. The data protection principles, outlined in these Guidelines, will remain relevant to the incoming Data Protection Reform with the revision of the Regulation[6]. One major change that is expected with these new rules is a greater focus on accountability, a shift that these Guidelines already anticipate (see paragraph 15 on accountability).

6. Annex IX of the Staff Regulations outline the rules for disciplinary proceedings in the EU institutions. These Guidelines focus on data protection principles. The procedural rules related to an administrative inquiry and a disciplinary proceeding are not analysed here.

2. THE LEGAL BASIS FOR AN INQUIRY

7. Administrative inquiries relate to a potential breach of a statutory obligation by a staff member. Personal information must be processed fairly and lawfully[7]. EU institutions and their investigators should be aware that personal information related to a suspicion of misconduct is by nature sensitive information.

8. The rules must be clear and transparent ex ante for everyone from an investigator to the person being investigated and the legal framework must be clearly defined. The Regulation allows the processing of personal information if the processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties[8]. This means that EU institutions, before carrying out an inquiry, should verify whether the inquiry can be based on a specific legal basis and whether it is necessary for the sound management and interest of the EU institution.

9. Article 86 of the Staff Regulations and their Annex IX set forth the legal basis of the disciplinary proceedings, but they do not provide a sufficiently detailed legal basis for the conduct of administrative inquiries. Therefore, in line with Article 2 of Annex IX[9], your institution should adopt a legally binding decision, policy or implementing rules regarding this procedure. This specific legal instrument should define the purpose of an administrative inquiry, establish the different stages of the procedure to be followed and set out detailed rules and principles to be respected in the context of an inquiry and a disciplinary proceeding. Furthermore, the rules about the use of different means in view of collecting potential evidence for the investigation should be included in the legally binding decision, policy or implementing rules (see paragraph 5 below).

---

[6] On 27 April 2016, adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council 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). It was published on 4 May 2016 in the Official Journal L119.

[7] See Article 4(1)(a) of the Regulation.

[8] See Article 5(a) of the Regulation.

[9] "*The rules set out in Article 1 of this Annex shall apply, with any necessary changes, to other administrative enquiries carried out by the Appointing Authority*" (para 1) and "*The appointing authority of each institution shall adopt implementing arrangements for this Article, in accordance with Article 110 of the Staff Regulations*" (para 3).

10. A specific legal instrument will then serve as a specific legal basis for administrative inquiries, which is missing so far. It will set out the process of an inquiry with legal certainty, safeguards and clarity in the interest of your institution. It should also give those implicated in the inquiry the necessary information about their rights and how to exercise them.

3. DEFINITION OF PERSONAL INFORMATION

11. Personal data or personal information is defined as any information that relates to an identified or an identifiable natural person[10]. 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[11]. This needs to be considered, for instance, when determining the scope of the affected individuals' right of access. In most cases, personal information includes identification data (i.e. contact details) but also data that relate to the behaviour of an individual.

12. The same piece of information may relate to different individuals at the same time. An administrative inquiry report includes information that identifies the person under investigation. The report may also contain personal data of the alleged victim, witnesses and third parties (persons merely quoted in the file).

13. 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 is about that individual.

Example 1: *An inquiry report may refer to the fact that a witness has been a reliable source of the inquiry. In such case, the whole report is not personal information relating to the witness. What can be considered information which is personal to the witness is only their name, their statements and the comment about reliability.*

4. CATEGORIES OF INDIVIDUALS INVOLVED

14. It is important to identify the different categories of individuals involved. In this way, it will be easier to establish their data protection rights and any possible limitations to these rights throughout the inquiry or disciplinary proceeding.

[10] Article 2(a) of the Regulation: " *'personal data' shall mean any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity*".

[11] WP29 4/2007 on the concept of personal information.

15. Standard categories usually include the person being investigated, witnesses, third parties (persons merely quoted in the file) and alleged victims (of psychological or sexual harassment for instance).

5. NECESSITY AND PROPORTIONALITY WHEN COLLECTING DATA

16. Investigators should apply rigorously the principles of necessity and proportionality when choosing the means of inquiry. The principle of data minimisation should be applied for all means and steps of the investigation, i.e investigators should limit the collection of personal information to what is directly relevant and necessary to the purpose of the inquiry and of the disciplinary proceeding. They should also retain the information only for as long as it is necessary to fulfil that purpose. In other words, investigators should collect only the personal data they really need, and they should keep it only for as long as they need it (see paragraphs 3 and 4 below).

17. Your institution should consult their DPO in this regard and take into consideration its DPO's practical guidance and advice. This will help your institution to better implement the principles of the Regulation and be accountable.

18. The data protection rules on the use of different means for collecting potential evidence for the investigation should be reflected in a Manual including specific guidance, which could be included in the general policy/decision/implementing rules.

19. The hearing of the person under investigation and of witnesses and victim is usually a proportionate option, as it is the least intrusive and the most transparent means to conduct an inquiry. Should a hearing be impossible, your institution should assess the level of intrusion to the individuals' privacy and use the least invasive means. The balancing exercise should be documented and it should take into account the following aspects:

- Your institution must evaluate how serious the misconduct under investigation is, to be able to judge whether more intrusive means of investigation would be justified, i.e. the acceptable intrusiveness of measures depends on how serious is the misconduct.
- The benefits derived from the use of specific means should outweigh the violation of privacy of the individuals.
- It must be ensured that there are no other alternatives to the use of intrusive means to successfully investigate the case.

20. **Hearing:** An initial interview with the affected individuals (person under investigation, witnesses, victims, etc.) is an appropriate method to obtain any information and establish the alleged facts or evidence relevant to the inquiry.

21. **Copy of paper information related to the inquiry:** when collecting paper information, investigators should consider blanking out irrelevant or excessive information to the inquiry.

22. **Copy of electronic information related to the person under investigation:** If this evidence is necessary and relevant to the inquiry, the IT service should be responsible for the technical aspects of its collection. The IT officers authorised to be involved should be strictly limited (need-to-know principle). The investigators' request should be specific so that the IT service will extract only specific and relevant information.

Example 2: *Investigators should identify relevant filters for the investigation up front and specify the subject matter, the relevant period, the expeditor's name and the recipient's name to the IT service.*

23. Below is a list of methods that can be employed to investigate serious offences[12]. They must be clearly stated in your institution's policy and they should be thoroughly regulated as they may be abused. The investigators should always conduct an assessment of necessity and proportionality before one of these means is used. This assessment should be duly documented before the investigation in order to allow judicial or administrative review in case it is contested.

24. **Covert surveillance:** In principle, video-surveillance systems should not be installed for the purpose of an inquiry, as it is highly intrusive since the person under surveillance is not made aware of its existence. Furthermore, it has little or no preventive effect and it may be abused as a form of entrapment to secure evidence. However, exceptional circumstances may justify its use. Your institution must have a published official policy on covert surveillance and its use should be subject to a privacy impact assessment. The policy on covert surveillance is subject to prior checking by the EDPS. The conditions under which the use of cover video surveillance may be justified are outlined in the EDPS Guidelines on CCTV[13].

25. **Traffic data**[14]**:** If your institution considers that internet connections and the use of e-mail or the telephone are necessary in the context of an inquiry:

- the investigators should establish a list of the traffic data they request to be collected;
- if such information is necessary to be processed for telecommunications budget and traffic management (i.e. an inquiry related to telephone traffic data of a staff member[15]) it can be kept for a maximum retention period of 6 months after

[12] For further information, see section 2.6 of the "EDPS Guidelines on personal data and electronic communications in the EU institutions" https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-16_eCommunications_EN.pdf.

[13] See page 31 of the EDPS Guidelines on video-surveillance of 17 March 2010, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

[14] See Article 37 of the Regulation.

[15] Practical experience has proved that it is difficult to make a distinction between traffic data relating to private use and traffic data relating to professional use. The fact that a particular phone call is

collection or even a longer period in order to safeguard an on-going investigation, or to establish or defend a right in a legal claim pending before a court[16]**.** This should be specified by referring to the closure of the investigation, i.e. 6 months after closure.

26. **Content of electronic communication:** The collection of evidence concerning the content of electronic communications in the course of an inquiry is subject to Article 36[17] of the Regulation, which deals with the confidentiality of communications. Any restriction of the confidentiality principle must be "in accordance with the general principles of Community law". The concept of "general principles of Community law" refers to the fundamental human rights under the European Convention on Human Rights (ECHR)[18] and in particular, to Article 8 (2) of ECHR[19] which provides four criteria to be examined before the principle of confidentiality is restricted:

- Is the restriction authorised by a legal provision or equivalent measure?
- Is it necessary? Could the same result be obtained without breaching the principle of confidentiality? It would only be in exceptional circumstances that the monitoring of a staff member's personal use of e-mail or telephone would be considered as necessary[20].
- Is it proportionate to the concerns it tries to address?

---

designated by the author as private is not *per se* a guarantee that it cannot be relevant for the investigations. The institution's policy should explicitly empower the investigators to collect traffic data without distinction between those marked as professional and those marked as private and the same standards should apply to both types of use.

[16] Article 20(1)(a) of the Regulation may be applicable, if the storage of traffic data constitutes a necessary measure to safeguard *"the prevention, investigation, detection and prosecution of criminal offences"*. Such provision should be subject to a strict interpretation.

[17] *"Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law"*.

[18] See also Article 7 of the EU Charter of Fundamental Rights, which is binding for EU institutions and bodies according to Article 6(1) TEU.

[19] See also Article 52 of the EU Charter of Fundamental Rights and in particular paragraph 3: "*In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection*".

[20] See Barbulescu v. Romania ECtHR judgment of 12 January 2016 (application no.61496/08). In this particular case, the company adopted an absolute ban on employee's use of work equipment for private reasons. Barbulescu's boss suspected that he was not complying with this policy, and informed him of its suspicions, on the basis of monitoring his account. The employee denied non-compliance, so the employer presented him with a transcript of his Yahoo messenger communications, which included personal communications. The employee argued that his employer violated his right to privacy under Article 8 of the ECHR, but the majority of the ECtHR disagreed with. The ECtHR held that the employer was simply trying to enforce its absolute ban on private use of work equipment, and he had breached his employment contract. The employer has only accessed the account to check whether he was using it just for professional purposes, given that he had claimed that he did not use for private reasons. There was no "reasonable expectation of privacy" under the company's specific policy.

- Have all other less intrusive means of investigation been exhausted?

6. RULES FOR PROCESSING SENSITIVE DATA

27. Personal information related to a suspicion of misconduct is by nature dealing with the processing of sensitive information and therefore your institution must adopt legally binding rules.

28. According to Article 10 (1) of the Regulation, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited unless one of the exceptions stipulated in Article 10 (2) of the Regulation applies.

29. In the course of an inquiry, investigators may collect sensitive information, such as data concerning health, e-mails exchanged by the affected individuals with trade unions or with the EU Sickness insurance scheme, information revealing political opinions etc. The exception that is usually applied in such cases, so that the general rule of prohibition of the processing of sensitive data may be lifted is Article 10(2)(b) of the Regulation. In principle, the processing of sensitive data in the context of an inquiry may be necessary in order to comply with the obligations and rights of your institution in the field of employment law insofar as it is authorised by EU law[21]. In these cases, the adoption of a specific legal basis for an inquiry is a pre-condition for the processing of sensitive personal data (see paragraph 2 above).

30. Inquiry files contain information relating to staff members' misconduct, which may fall under the concept of offences, criminal convictions or security measures, as the Regulation refers to explicitly. Processing of such data is subject to authorisation under Article 10(5) of the Regulation. This is an additional reason why your institution should adopt a legal instrument before launching an inquiry (see paragraph 2 above).

31. In any event, your institution should ensure that the investigators, responsible for an inquiry, are fully aware of the restrictions, which apply when processing sensitive information.

7. DATA QUALITY

32. Furthermore, your institution should ensure that investigators apply the principle of necessity and proportionality when collecting personal data[22] as the Regulation requires them to do.

---

[21] Article 10(2)(b) of the Regulation provides that Article 10(1) shall not apply where the processing is *"necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof"*.

[22] Article 4(1)(c) of the Regulation states that *"personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"*.

33. On one hand, investigators should limit the collection of personal information to what is directly relevant and necessary to the purpose of their inquiry or disciplinary proceeding. On the other hand, they should erase any information, which is excessive and no longer necessary to the purpose of the inquiry or disciplinary proceeding.

34. Although certain standard administrative data, such as name and date of birth are always recorded in the inquiry files, there is no systematic rule regarding the nature of data, which can be included in an inquiry file; the precise content of a file will vary according to the nature of the particular case.

35. In the course of an investigation, investigators may come into possession of personal information, which is of no interest or relevance to the investigation. Any such information should be promptly erased and not further processed. This is particularly important for special categories of data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life (see paragraph 3).

8. ACCURATE AND UP TO DATE DATA

36. Personal data must be accurate and kept up-to-date[23]. Your institution should ensure that any inaccurate or incomplete information is erased or rectified in light of the purpose of the inquiry or of the disciplinary proceeding.

37. In order to understand the principle of accuracy in this context, it is important to make a distinction between **"hard"** and **"soft"** data, as this will play an important role in the application of the right of rectification:

- Data qualified as **"hard"** or "objective" are factual, administrative information including identification data relating to those implicated in an inquiry or procedure;
- Data qualified as "**soft**" or "subjective" are allegations and declarations by the affected individuals, which may also be based upon a reasonable suspicion or the subjective perception of the investigators. In some cases, they are not verifiable.

38. The accuracy of soft data in the context of an inquiry or disciplinary proceeding therefore means whether the statement that was made has been accurately recorded and not misinterpreted. Nevertheless, your institution should ensure that the inquiry/disciplinary file is kept as accurate and complete as possible. The individuals involved should be in a position to verify that their hard data are accurate and up to date. As to the accuracy of the soft data and the completeness of the inquiry/disciplinary file, the following measures must be taken:

a. **draft administrative inquiry/disciplinary report*:*** the person under investigation should be entitled to comment on the facts concerning them. They

[23] Article 4(1)(d) of the Regulation states that personal data must be *"accurate and, where necessary, kept up to date"; "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified".*

should be sent a summary of the facts and preliminary conclusions and be allowed to send comments within a specific deadline.

b. **record of a hearing*:*** in principle, statements should be signed once the interviewee has had sufficient time to read and correct the statement. If this is not possible, the interviewee could be sent the record of the hearing by registered letter with acknowledgment of receipt, for signature. They then should forward the signed letter and any comments and remarks within a specific deadline.

c. **all documents related to an inquiry/disciplinary proceeding (including the above documents):** should be kept in the inquiry/disciplinary file for accuracy and completeness of the file.

9. INFORMATION TO ALL INDIVIDUALS INVOLVED

9.1. General information about administrative inquiries and disciplinary proceedings

39. Your institution should inform all individuals implicated in an inquiry or disciplinary proceeding of the main data protection principles. This can be done, for example, by posting a privacy notice where they have published (i.e. intranet) all the relevant documents about administrative inquiries and disciplinary proceedings (Decision, Rules, Policy, Manuals). This privacy notice should refer to all relevant information related to administrative inquiries and disciplinary proceedings in general following the list of elements stated in Articles 11 and 12 of the Regulation.

9.2. Specific information to affected individuals (Articles 11 and 12 of the Regulation)

40. The data protection notice mentioned above is a first step, but it is not sufficient. Personal data must be processed fairly[24]. In order to guarantee fairness and transparency about the information processed regarding a specific inquiry, affected individuals should be informed about it. Your institution should therefore provide them with the privacy notice as soon as it is practically possible, for example before starting the interview of the person. In principle, your institution should inform them of the opening and closing of the administrative inquiry related to them. This concerns the formal opening of an inquiry as well as the following stage, when the available information will either be transferred to a Disciplinary Board appointed by your institution or to IDOC, or to its equivalent for a disciplinary proceeding (see further paragraph 12 on "transfers").

Article 11(1)(d) of the Regulation

[24] See Article 4(1)(a) of the Regulation.

41. The data protection notice should outline the possible consequences of hindering the administrative inquiry; for instance, if the witness maliciously makes a false statement, disciplinary measures could then be a possible consequence of their malicious act.

9.3. Restricting information to the person under investigation(s) (Article 20 of the Regulation)[25]

42. In some cases, informing the person under investigation about the inquiry or the disciplinary proceeding at an early stage may be detrimental to the investigation. In these cases, your institution might need to restrict the information to the person being investigated to ensure that the inquiry or disciplinary proceeding is not jeopardised[26].

43. Your institution should inform the person under investigation of the principal reasons on which the application of the restriction is based as well as of their right to have recourse to the EDPS[27]. In some specific circumstances, it might be also necessary to defer the provision of such information so that the investigation process will not be harmed[28].

44. Your institution should therefore indicate in a data protection notice that the right to information may be restricted on a case by case basis depending on the specific inquiry or disciplinary proceeding.

How are Articles 20(3) and 20(5) of the Regulation applied in practice?

In cases where your institution decides to apply a restriction of information, access, rectification etc. under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4), such decision should be taken strictly on a case by case basis. In both cases, your institution should be able to provide evidence demonstrating detailed reasons for taking such decision (i.e. motivated decision). These reasons should prove that they cause actual harm to the investigation or they undermine the rights and interests of your institution and they should be documented before the decision to apply any restriction or deferral is taken. The documented reasons should be made available to the EDPS if requested in the context of a supervision and enforcement action.

[25] Article 20(1(a) of the Regulation should be interpreted in light of Article 13(d) of Directive 95/46/EC including breaches of ethics for regulated professions.
[26] See Article 20 of the Regulation regarding the exemptions and restrictions.
[27] See Article 20(3).
[28] See Article 20(5).

10. RIGHT OF ACCESS AND RECTIFICATION TO ALL INDIVIDUALS INVOLVED

10.1. Right of access

45. In principle, affected individuals have the right to contact your institution and request access to their personal information. They have the right to be informed about any information relating to them that is processed by your institution. Access is essential in order to allow affected individuals to exercise their right of defence as well as their rights under the Regulation.

10.1.1. Possible restrictions to the right of access

46. In specific circumstances, it may be necessary to restrict the right of access of the **person under investigation** or **alleged victim** but also of a **witness** under one of the exemptions of Article 20(1) of the Regulation. If Article 20 applies, check paragraph 8 above.

Example 3: *A person under investigation regarding harassment may experience a limitation to his/her right of access in order to protect the alleged victim.*

Example 4: *The right of access of a person under investigation to the identity of a witness should be restricted in order to protect the witness' rights and freedoms.*

47. Those being investigated and alleged victims should have full access to the final decision of an inquiry or a disciplinary proceeding. However, the right of access of a witness to the final decision should be stricly assessed on a need-to-know basis; it is possible that the final decision in the end does not include personal data of a witness; it would thus be out of scope for a request for access from that person.

48. Any decision for a restriction of the right of access or for deferral should be taken strictly on a case by case basis and the reasons of the decision should be documented, as explained in paragraph 9.3, last point).

10.2. Right of rectification

49. To exercise the right of rectification, affected individuals should contact your institution directly via a specific functional mailbox[29] allowing written requests and confidentiality. Your institution should be able to guarantee the right of rectification when affected individuals exercise it, so that their files are complete and kept up to date (see also paragraph 8 on "accuracy").

50. The right of rectification of "soft" data means that your institution should allow individuals to add their comments to their file related to the inquiry and include

[29] Affected individuals should be able to contact directly the EU institution in order to be able to exercise their rights.

additional testimonies, or other relevant documents (i.e. legal recourse or appeal decision). In addition, the final decision should be placed in the personal file of the affected individual and where appropriate, it should be replaced or removed.

10.2.1. Possible restrictions to the right of rectification

51. In case a restriction to the right of rectification is necessary, the same principles as to the right of information and of access are applicable.

11. RETENTION PERIODS DEPENDING ON OUTCOMES OF CASES

52. Personal data must not be kept longer than necessary for the purpose for which they are collected or further processed[30].

53. Your institution should make a distinction between the following scenarios:

a. **Pre-inquiry file:** When your institution makes a preliminary assessment of the information collected and the case is dismissed. In such cases, your institution should set up **a maximum retention period of two years** after the adoption of the decision that no inquiry will be launched. This maximum retention period could be necessary for audit purposes, access requests from affected individuals (i.e from an alleged victim of harassment) and complaints to the Ombudsman.

b. **Inquiry file:** When your institution launches an inquiry including the collection of evidence and interviews of individuals, there could be three possibilities: *i) the inquiry is closed without follow-up, ii) a caution is issued or iii) the Appointing Authority of your institution adopts a formal decision that a disciplinary proceeding should be launched.* For cases i) and ii), **a maximum of five-year-period** from closure of the investigation is considered to be a necessary retention period, taking into account audit purposes and legal recourses from the affected individuals. For case iii), your institution should transfer the inquiry file to the disciplinary file, as the disciplinary proceeding is launched on the basis of the evidence collected during the administrative inquiry.

c. **Disciplinary file (in cases where the EU institution is in charge of the disciplinary proceeding):** Your institution carries out a disciplinary proceeding with the assistance of internal and/or external investigators on the basis of a contract. You should take into consideration the nature of the sanction, possible legal recourses as well as audit purposes and set up **a maximum retention period**, after the adoption of the final Decision. If the staff member submits a request, under Article 27 of Annex IX to the Staff Regulations, for the deletion

[30] Article 4(1)(e) of the Regulation: *"personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or for which they are further processed"*.

of a written warning or reprimand (3 years after the Decision) or in the case of another penalty (6 years after the Decision, except for removal from post) and the Appointing Authority grants the request, the disciplinary file which led to the penalty should also be deleted. If the Decision on the penalty stored in the personal file is deleted, there is no reason to keep the related disciplinary file. In any case, your institution could grant the possibility to the affected individual to submit a request for the deletion of their disciplinary file 10 years after the adoption of the final Decision. The Appointing Authority should assess whether to grant this request in light of the severity of the misconduct, the nature of the penalty imposed and the possible repetition of the misconduct during that period of 10 years.

d. **Disciplinary file (for which IDOC is in charge of the disciplinary proceeding):** Your institution concluded a SLA with IDOC to carry out the disciplinary proceeding and you therefore transfer the evidence collected to IDOC. Your institution should adopt a retention period in light of the outcome of the disciplinary proceeding carried out by IDOC; as soon as IDOC adopts its final Decision and conclusions, all information kept by your institution before their transfer to IDOC, should be erased.

11.1. Storage

54. There should be a distinction between the **personal file** and **the inquiry and/or disciplinary file.** Your institution is reminded that a copy of the disciplinary decision should be stored in the **personal file** of the affected individual taking into account the provisions of Article 27 of Annex IX to the Staff Regulations concerning a request for deletion of such data. Duplication of information in both, the personal and the inquiry/disciplinary file should be avoided, as it would be detrimental to the legitimate interests of the staff member.

55. Your institution should also ensure that, when the Appointing Authority decides to close the case without imposing any disciplinary penalty, there should be no traces of the final decision in the personal file, unless the staff member so requests (Article 22 of Annex IX to the Staff Regulations). Such a practice is beneficial to the staff member's interests, as it will avoid leaving any unnecessary traces which might raise some suspicions or other sorts of implications towards a staff member's innocence.

The distinction of the different categories of retention periods should be specified in a Manual included in the specific legal instrument.

12. TRANSFERS OF DATA

12.1. Internal transfer

56. Any transfer of personal data to recipients within or to other EU institutions must comply with specific requirements[31].

57. Transfers of personal information within the EU institutions may only take place as long as they are necessary for the performance of the recipients' tasks and competences and should occur on a strict need-to-know basis.

In case your EU institution, needs to transfer information within your own institution or to another EU institution[32]

58. You need to assess two issues: whether the receiving institution is **competent** or not and whether the personal data are **necessary** for the execution of the tasks of the receiving EU institution[33].

59. As to the issue of **necessity**, you should assess what information is needed to be transferred to the receiving EU institution and strictly limit the information transferred on the basis of this assessment. You should not transfer the whole file, but only the personal information, which is necessary and relevant to the tasks of the receiving EU institution.

In case an EU institution requests a transfer of information from your EU institution[34]**.**

60. Both parties should bear the responsibility for the legitimacy of the transfer. Your institution should make a provisional evaluation, taking into consideration the specificities of the case. This evaluation should consider the request and transfer to the requesting EU institution what is relevant and necessary to the request (data minimisation principle).

[31] *"Without prejudice to Articles 4,5,6 and 10, personal data shall only be transferred within or to other EU institutions, if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient".*
[32] Article 7(1) of the Regulation.
[33] For instance, IDOC has a specific investigative mandate to carry out an administrative inquiry and a disciplinary proceeding.
[34] Article 7(2) of the Regulation.

Example 5: *The investigators of an EU institution (A) submit a request to another EU institution (B) asking for the medical expenses' claims of Ms X in the context of an inquiry. B should not simply transfer the medical expenses of Ms X to B, as the medical expenses might include information on Ms X's spouse and children, which are not relevant to the purpose of the inquiry. If B is not certain about the information requested, or A did not specify the exact information needed, B should ensure that the information to be transferred is clear and precise; B should limit the content of the transfer of information to A only to the information that has been explicitly requested and not disclose other irrelevant information on other individuals.*

12.2. External transfer

61. In the cases where transfers of data to national authorities (such as national Courts) (subject to Regulation (EU) 2016/679), are required, your institution should offer specific guidance procedures in order to justify and document the **necessity of a transfer** under **Article 8(a)** of the Regulation:

- if information is transferred at the request of a national authority, the latter should establish the "necessity" for the transfer;
- if information is transferred on the sole initiative of your institution, it will be for the latter to establish the "necessity" for the transfer in a reasoned decision.

62. Finally, in cases where data related to an inquiry or a disciplinary proceeding, are transferred to recipients in countries that have not implemented a comprehensive data protection framework for judicial activities, **Article 9** should apply. In such cases, the Council of Europe Convention 108 is applicable to judicial authorities, which is to be considered as an adequate legal instrument for intra EU transfers in the field of judicial activities. This Convention is in principle[35] to be considered as adequate for the very specific intra EU transfers under analysis. Your institution should consider this aspect in their guidance and procedure.

13. CONTRACTUAL OBLIGATIONS WITH A PROCESSOR

63. Article 23 of the Regulation stipulates the role of the processor and the obligations of the controller in ensuring sufficient guarantees and compliance with technical and organisational security measures.

64. In light of **Article 23(a)** of the Regulation, your institution is responsible for determining the purposes and means of a processing[36]. An individual expert (i.e. a

[35] See the list of possible declarations of Contracting Parties under Article (3) (2) (a) of the Convention in: http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=&DF=&CL=ENG&VL=1.

[36] See Article 2(d) of the Regulation.

specialised doctor, a graphologist, a former judge, a former staff member specialised in Staff Regulations etc.) who is part of the members of an inquiry panel or a Disciplinary Board, will be classified as a processor[37]. As such, they are obliged to carry out the processing only on instructions from your institution. This means that your institution, being the controller[38], should indicate in the contract with its processor, specific terms and conditions so that the processing of data related to an inquiry/disciplinary proceeding is carried out lawfully in conformity with data protection rules (i.e. purpose limitation, data quality, retention periods, prohibition of data transfer for incompatible purposes etc.).

65. As to the obligations of the processor regarding confidentiality, data protection and security measures under **Article 23(2)(b)** of the Regulation, your institution should ensure that specific provisions are added in the legal act/contract regarding these obligations. As to the confidentiality and security obligations, if the processor is subject to the national law of a Member State, it should in principle be bound by Article 28 of Regulation (EU) 2016/679, implemented in the Member State's national law on data protection (see further in paragraph 14 on "security").

14. SECURITY MEASURES

66. Special care must be taken to ensure the security of the personal data that are collected, processed and stored. Given that the information processed is sensitive, leaks or unauthorised disclosure of it may have severe consequences for all individuals involved in an inquiry or procedure. Article 22 of the Regulation requires your institution to implement appropriate technical and organisational security measures in view of preventing any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

67. In practice, this means that your institution should carry out a risk assessment of their already existing general security policy within their premises and develop, where necessary, specific security measures on access control and management of all the information processed in the context of an inquiry or disciplinary proceeding.

14.1. Technical measures

68. Your institution should develop, document and implement an access review and logging policy with a description of i) the list of authorised categories of officers who have access to the drives shared between the units involved in an inquiry/disciplinary proceeding, ii) what information is logged in the drives, iii) what use is made of the logged information and iv) the process in place to review the access rights. This policy is important in order to allow your institution to ensure that throughout an inquiry or

[37] Article 2(e) of the Regulation: "*'processor' shall mean any natural or legal person, public authority, agency or any other body which process personal data on behalf of the controller*".
[38] See Article 4(2) of the Regulation.

disciplinary proceeding, only authorised officers are attributed access rights and only on a "need-to-know" basis.

14.2. Organisational measures

69. Due to the sensitive nature of the data processed, all officers involved should sign confidentiality declarations stating that they are subject to an obligation of professional secrecy equivalent to that of a health professional. These declarations will contribute in maintaining the confidentiality of personal data and in preventing any unauthorised access within the meaning of Article 22 of the Regulation. This is an example of the measures that your institution should take to promote a data protection culture among officers involved in an inquiry or disciplinary proceeding.

15. INVOLVEVEMENT OF THE DPO WHEN NECESSARY

70. Your institution should ensure that the specific legal basis, analysed in paragraph 1, contains provisions regarding the role of the DPO. For instance, it must be stipulated that the DPO should be consulted regarding the choice of the means of investigation or when restrictions of the rights of affected individuals are envisaged. By involving their DPO early in the process, the DPO will be able to offer to your institution valuable advice and guidance. It should be clear that the DPO's concrete involvement and advisory role is not merely a formalistic requirement but a necessary complement of the procedure.

16. ACCOUNTABILITY

71. Accountability means that your institution must ensure compliance with its data protection obligations and it must **be able to demonstrate that it does so** upon request.

72. Accountability is not specific to personal information within these procedures, but it applies to all operations that process personal information.

73. Your institution that collects, uses and stores (collectively known as processing) personal data is responsible and accountable for complying with data protection rules.

74. In general, your institution must be transparent and explicit about how it processes the personal information. It must document its 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. Your institution cannot assume that staff will know.

75. Different processing operations and different technologies require different safeguards. The best way for your institution to be accountable is for it to be **proactive at all levels** and consider the data protection implications of new processing operations at the design stage **(data protection by design**): Your institution should

- Build a data protection culture into its **top level risk management** considerations; top level managers should have regular contacts and updates with the **DPO**[39] on the strategic and overall state-of-play regarding data protection.

- Ensure that the **DPO** is on board at the early stage of any policy developments in close cooperation with **the high level management;** High level managers should have regular contacts and updates on the state-of-play regarding their projects and where required, receive training on data protection issues. They should consider any potential risk of public procurement, liability and reputational damage due to the absence of data protection rules.

- Develop close contact between the **staff and the DPO**; Staff should have regular information sessions and trainings with their DPO about their data protection rights and related issues.

76. The questions listed below outline the main issues to consider:

    a. **Legal instrument:** Have you adopted a legal instrument on which an inquiry may be lawfully launched?

    b. **Specify and use proportionate means of collecting evidence:** Are the means proportionate? Are they reflected in a Manual included in the specific legal instrument?

    c. **Avoid excessive information:** What information is necessary and relevant for the investigation?

    d. **Identify the meaning of personal information:** What is personal information in the "hard" and "soft" data collected?

    e. **Inform each category of individuals:** Who are affected by this specific inquiry or disciplinary proceeding?

    f. **Apply specific retention periods:** How long do you need to keep the information collected before an inquiry, during an inquiry and in the context of a disciplinary proceeding? Are these retention periods specified in a Manual included in the specific legal instrument?

    g. **Conclude a contract with your processor:** If a processor (specialised expert) is necessary, does the contract stipulate the purpose of the outsourcing, the data protection principles and security obligations incumbent on the processor?

    h. **Conduct a risk assessment:** What are the risks an inquiry or disciplinary proceeding may present and how are you going to protect yourself from them?

77. **Accountability** also implies **documentation of the procedure** and implementation of the rules, and principles. The following should be documented and implemented:

    a. **A legally binding decision**, policy or implementing rules on an administrative inquiry;

[39] The Data Protection Coordinators in the big institutions should also be involved.

b. **A Manual of guidance** on the means of collecting evidence for the investigation;

c. **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;

d. **Any deferral of information** to the affected individual;

e. **A contract with a specialised expert**;

f. **The risk assessment** conducted for this specific procedure.

17. READ MORE AND COURT CASES

EDPS most recent prior-check Opinions

- Opinion of 19 December 2014 on notifications concerning the *"processing of administrative inquiries and disciplinary proceedings" by six Executive agencies*, cases 2013-1022 (REA), 2013-1012 (CHAFEA), 2014-0136 (INEA), 2014-0723 (EACEA), 2014-0805 (ERCEA) and 2014-0937 (EASME).

- Opinion of 22 June 2011 on notifications concerning the "processing of administrative inquiries and disciplinary proceedings" by five decentralised EU agencies, case 2010-0752.

EDPS Guidelines

- Guidelines concerning the processing of personal data during the selection of confidential counsellors and the informal procedures for cases of harassment in European institutions and bodies, 18 February 2011.

- Guidelines on processing personal information within a whistleblowing procedure, 18 July 2016.

- Guidelines on personal data and electronic communications in the EU institutions (eCommunications guidelines), 16 December 2015.

- Guidelines on the protection of personal data in mobile devices used by European institutions (Mobile devices guidelines), 17 December 2015.

- Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001, 21 March 2016.

Interception of communications

- Barbulescu v. Romania, ECHR judgment of 12 January 2016 (application no.61496/08).

- Halford v. The United Kingdom, ECtHR judgment of 25 June 1997 (application no.20605/92).

- Copland v. The United Kingdom, ECtHR judgment of 3 April 1997 (application no. 62617/00).

Rights of affected individuals

- Maria Concetta Cerafogli v European Central Bank, Judgment of the General Court (Appeal

Chamber) of 23 September 2015, case T-114/13P.

- AQ v European Commission, Judgment of the Civil Service Tribunal (Second Chamber) of 21 October 2015, case F-57/14.

- AX v European Central Bank, Judgment of the Civil Service Tribunal (Second Chamber) of 13 December 2012, case F-7/11.