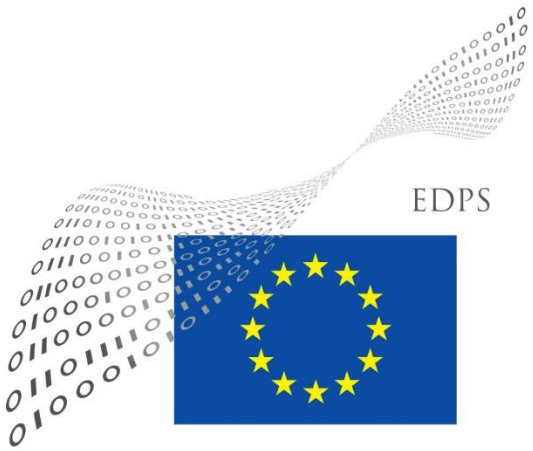
EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on personal data and electronic communications in the EU institutions



February 2020

Executive Summary

For most people, electronic communications (eCommunications) such as email, internet and telephony, occupy a central role in their day-to-day professional and personal activities.

Indeed today, eCommunications are essential for organisations to operate efficiently and the EU institutions, bodies, offices and agencies (EU institutions) are no exception.

These guidelines are intended to provide practical advice and instruction to the EU institutions on the processing of personal information in the use of eCommunications tools, to ensure that they comply with their data protection obligations as set out in the Data Protection Regulation (EU) 2018/1725 applicable to the EU institutions (Regulation).

In principle, organisations using eCommunications process the personal data of their employees, for instance, in the management of eCommunication services, billing and verifying authorised use. In most cases, a limited private use of work equipment is permitted, so interference by an employer on the use of eCommunications by employees is likely to touch upon aspects directly relating to their private lives.

Therefore, eCommunications is a complex subject and requires guidance. The domain is also one of the most dynamic fields of technology and is subject to rapid change. As a consequence, these guidelines take a technology-neutral approach and do not prescribe specific technical measures. Instead, they put a clear emphasis on the general principles of data protection that will help EU institutions comply with the data protection Regulation.

While these guidelines are in principle aimed at the EU institutions, anyone or any organisation interested in data protection and eCommunications might find them useful: the Regulation is similar in many respects to the General Data Protection Regulation (GDPR) applicable to organisations in the EU/EEA.

These guidelines update an earlier text on the same topic issued in December 2015.

Summary of Recommendations

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

Recommendations for specific processing operations:

On systems security and traffic management:

R1: Define the content of security logs and their conservation periods according to the security needs of your institution

R2: Data collected for security monitoring purposes must *only be used for those* purposes

R3: Ensure that statistics generated are anonymous.

R4: Make sure that eCommunications are encrypted to the highest standards and update to state-of-the-art encryption schemes.

On billing and budget management:

R5: Instruct external providers to minimise the amount of personal data provided to the institutions for billing purposes wherever possible

R6: Define conservation periods based on the periods for contesting invoices

On authorised use of eCommunications services:

R7: Adopt a progressive approach towards monitoring the authorised use of eCommunications Services.

On the recording of dedicated phone line:

R8: Adopt an administrative measure detailing how and why phone calls need to be recorded

R9: Inform both callers and staff about the (possible) recording of phone calls *before* it happens.

On access to emails in the absence of the employee:

R10: Take precautionary measures to reduce the need for accessing personal mailboxes for business continuity purposes

R11: Adopt a policy on accessing the mailboxes of absent staff if there is a business need.

On administrative enquiries and disciplinary proceedings

R12: Make sure that access to eCommunications data is covered under the rules for administrative inquiries and disciplinary proceedings

R13: Provide adequate safeguards when planning covert surveillance, including internal rules under Article 25 of the Regulation.

TABLE OF CONTENTS

1. INTRODUCTION

1 These guidelines are intended to provide practical advice and instruction to the EU institutions on the processing of personal data in their use of eCommunications tools, to ensure that they comply with their data protection obligations as set out in Regulation (EU) 2018/1725 (the Regulation).

2 These guidelines build on previous EDPS decisions and Opinions (on administrative consultations, complaints and past prior checks), as well as on the work done by the Article 29 Working Party (WP29) and then by the European Data Protection Board which replaced it. Given that the terms and concepts used in the rules applicable at national level and for the EU institutions are largely similar, the EDPS follows the interpretation of them by the WP29 and EDPB wherever appropriate. Where we do not take a position, the EDPS takes the one defined in these other documents.

3 The EDPS has developed these guidelines based on long-term experience. A first edition was published in December 2015; in the meantime, the data protection rules applicable to the EU institutions have evolved with the replacement of Regulation (EC) 45/2001 with Regulation (EU) 2018/1725, which mirrors the General Data Protection Regulation (GDPR) applicable to organisations in the EU/EEA. This new edition updates the guidance provided to account for that change and to cover new issues. Conversely, the chapter on general recommendations has been removed, as its substance is now covered in other guidance documents.

4 By following these guidelines you can be reasonably assured that you comply with the Regulation within the scope outlined. The EDPS will use these guidelines as a standard by which to assess your compliance.

5 If you are using these guidelines as an IT or other service of an EU institution, your first point of contact for further guidance will be your data protection officer. Every European institution, body and agency has at least one and they will be able to provide further guidance.

6 As well as being of specific interest to data protection officers, data protection coordinators, IT and other services, these guidelines could be of interest to any persons who use the eCommunications resources of the EU institutions (all categories of staff, MEPs, delegates of member states, contractors, visitors, etc.).

2. SCOPE AND RELATION TO OTHER EDPS GUIDANCE DOCUMENTS

7 In line with the scope of application of the Regulation, these Guidelines apply to processing *by* the EU institutions. In most cases, the users concerned will be staff (defined broadly and includes for example seconded national experts, trainees and on-site-contractors), but they can also be persons external to the institutions (e.g. for guest access to internet). While the specific rules in place for different categories of persons may differ (e.g. administrative enquiries for those persons subject to the Staff Regulations and those who are not), the principles are the same. In summary, the guidelines apply when eCommunications data concerning all these categories of data subjects are processed *by* EU institutions, without prejudice to a separate or specific policy that the EU institutions may consider with regard to their high level or political representatives.

8 The following categories of eCommunications are covered by these guidelines:

- telephony;
- email; and
- internet.

9 Because technology evolves quickly, the specific tools and means used to provide these services may change. However, the general principles apply. Therefore, our guidance has been drafted to be as technologically neutral as possible.

10 The guidelines deal with the processing of personal data generated by eCommunications for the following purposes:

- billing and budget management;
- security and traffic management;
- incident management and troubleshooting;
- verification of authorised use of eCommunications systems;
- recording of specific telephone lines (e.g. emergency lines);
- access to eCommunications data of an employee in his/her absence;
- administrative investigations and disciplinary proceedings (AI&DP).

11 These Guidelines do NOT apply to:

- identity and access management systems;
- monitoring by means of video-surveillance;
- remote sessions on the organisation's network;
- user activity monitoring systems (such as productivity monitoring);
- local storage (i.e. storage of files on local drives);
- user to user and user to server communications on the organisation's network (e.g. instant messaging between colleagues, access to internal websites etc.);
- institutional public web sites;
- processing of personal data of third parties when using mobile devices;

- processing of personal data by mobile apps offered by EUIs.

12 Processing eCommunications data is the processing of personal data, so other EDPS guidance documents will be relevant too[1]:

- On how to document your processing operations, as well as how to conduct data protection impact assessments and proceed to prior consultation of the EDPS (where necessary), see our guidance on Accountability on the ground;
- On how to integrate data protection aspects into your IT governance processes, see our Guidelines on IT governance and IT management;
- Take extra care when outsourcing processing operations, as this may make it more difficult for you to control data flows[2].

Rx: Recommendations are highlighted in boxes accompanied by further explanation below each box

13 For actions that are mandatory, our recommendation is to use the appropriate language to indicate an obligation: “have to", "do this", "you must" or other imperative forms.

14 Similarly, for actions that are recommended as good practice, but are not obligatory use "You should", "ought to" and so on.

15 "May", "could" and similar wording refer to actions that are voluntary or that are equally valid ways of achieving the same goal.

16 For practical purposes, EU institutions, bodies and agencies will be referred to as 'institution', 'your institution', or 'your agency' throughout these guidelines but are equally applicable to all.

3. RECOMMENDATIONS FOR PROCESSING PERSONAL DATA FOR SELECTED eCOMMUNICATIONS

3.1. Systems Security and Traffic Management

17 Your institution's eCommunications may require some monitoring to ensure that they function the way that they should. This includes processing operations which aim to:

- ensure the security and stability of the systems;
- detect and prevent attacks (internal and external);

[1] The 2015 version of these Guidelines included a part on general recommendations that would apply to any kind of processing of personal data as well. For this kind of general information, refer to the Accountability on the ground toolkit.

[2] See EDPS letter on the application of data protection clauses in EUI contracts of 23 May 2019, available here: https://edps.europa.eu/data-protection/our-work/publications/consultations/application-data-protection-clauses-eui_en, and EDPS letter on a consultation concerning updating service contracts, available here: https://edps.europa.eu/data-protection/our-work/publications/consultations/consultation-concerning-updating-service_en

- ensure the proper functioning of the systems;
- measure usage.

18 Some internet monitoring may also be necessary to ensure network functionality (control) and security.

R1: **Define the content of security logs and their conservation periods according to the security needs of your institution**

19 You must limit internet monitoring for security and traffic management purposes to what is adequate and relevant for the purposes of the processing (see Annex 1 for further explanation on the principle of data quality). In practice, this means:

- using other less intrusive tools or technologies wherever possible (such as the blocking of web pages) and limiting the generation of logs accordingly;
- limiting the personal information recorded in the logs to that which is absolutely necessary;
- defining a limited period for retaining the logs.

20 For example, internet access logs usually include (per use and per internet access attempt):

- a user identification and IP address;
- the volume of data exchanged with the internet;
- the date and time of the access.

21 Similarly, storing email traffic data may be necessary for the same purposes. The following fields are most frequently included by the EU institutions and may be a useful reference for your organisation:

- From:
- Date:
- Message-ID:
- To:
- Subject:
- Bcc:
- Cc:
- Content-Type:
- Sender:

22 **Conservation periods**: personal data must not be kept for longer than is necessary for the purposes for which it was collected or further processed (Article 4(1) (e) of the Regulation). Once you have defined the purpose and the type of data you need, you must define how long you will keep it. This applies both to your internal networks used by your staff and to guest networks that your visitors can use.

R2: **Data collected for security monitoring purposes must *only be used for those* purposes**

23 The general principle of **purpose limitation** (see Annex 1) restricts the further use of personal data. Article 6 of the Regulation explains the concept of 'compatible use' in further detail.

24 **Email screening** for the purpose of eliminating viruses or other malware as well as spam is one example of processing for "security and control" purposes. It is based primarily on filtering email traffic data (volume, type of attached files, email headers, etc.) but automated content filtering is also possible, especially in the case of spam and detection of predetermined content. Although the processing is performed automatically by means of specific software tools, manual intervention by the system administrator may be needed in specific cases if justified.

Example 1: *Spam filtering*

Your institution filters incoming emails to avoid spam. However, staff have complained that the system fails to detect certain spam messages (false negatives), while blocking some legitimate messages (false positives).
In order to fine-tune the system, a system administrator has to look at the content of the messages flagged by members of staff. In this case, a manual intervention may be justified, while during normal operations, administrators should not look at the content but rely on the automatic filtering.

R3: **Ensure that statistics generated are anonymous**

25 When internet access logs are (automatically or manually) further analysed for **producing statistics** and evaluating your institution's internet usage (for example, by the Security Officer or other administrative departments), the data should be made **anonymous**. While the generation of these statistics may involve the processing of personal data, the **results must be anonymous**.

R4:**Make sure that eCommunications are encrypted to the highest standards and update to state-of-the-art encryption schemes.**

26 Encryption of eCommunications has been recognised as a must-have control. The objective is to minimise the risk that, if traffic is intercepted, it is in an unintelligible form.

27 However, the field of cryptography (the study of encryption/decryption and attacks to break encryption) is ever evolving. Coupled with the fact that technological advances increases raw computing power that can be used to attack encryption mechanisms, the future is looking bleak for the robustness of those encryption mechanisms. For example, the advent of quantum computing, which at the time of writing is still in its infancy, will be a game-changer for the assurance of confidentiality that encryption mechanisms provide.

28 The most advanced encryption schemes and configuration of these encryption schemes should be implemented for all eCommunications. Furthermore, continuous updates to state-of-the-art encryption schemes is a must so as to assure the maximum level of confidentiality for information sent over a network.

3.2. Billing and Budget Management

29 Your institution may need to process personal data for the billing and budget management of eCommunications services such as itemised invoices for phone calls.

30 Data processed for the monitoring of billing and invoices **have to be limited to what is necessary** (as per the data quality principle, see Annex 1). The following data is generally considered adequate for monitoring fixed line and mobile phone calls:

- phone extension name;
- phone extension number;
- numbers called (the last three digits should be removed to ensure privacy if the provider offers this option);
- date, time and duration of each call;
- amounts charged;
- volume of data exchanged (for mobile internet access).

31 In contrast, the **identity of the person called**, **unsuccessful call attempts**, **unanswered calls**, **received calls** and **specific web sites** visited **do not need to be recorded for billing purposes**. This does not affect the potential need to keep records of missed/placed calls locally on the phone itself.

R5: **Instruct external providers to minimise the amount of personal data provided to the institutions for billing purposes wherever possible.**

32 The information needed for billing and budget management is usually received from the eCommunications provider together with the invoices (for telephony) or generated by your institutions' own IT infrastructure (for internet and email traffic data). It is for your institution to instruct the provider to restrict the categories of data included in the associated invoices wherever possible.

33 Not all data fields mentioned in 3.1 above are relevant for both billing and budget management. For example, email traffic data is likely to be irrelevant for billing, while the volume of data exchanged with the internet may be relevant where access is billable by volume on smartphones. Only the fields essential for billing and budget management should be stored and used.

R6: **Define conservation periods based on the periods for contesting invoices.**

34 The period of time you plan to store call records or other logs (the conservation period) for the purposes of budget management and billing purposes should not exceed the period that is allowed for contesting bills for communication services (see Article 36 of the Regulation . The periods for contesting bills may vary according to the contracts

your organisation has with the providers of communications services and the conservation periods should be set accordingly (see also Annex 1 on not keeping personal data for longer than is need).

35 If you need to keep some data for a longer period, for example because of financial rules or for auditing purposes, **access should be restricted** to those roles directly involved in these tasks.

36 The reasoning in the preceding two points also applies if your institution allows staff to use communications equipment for private use and bills them for this use.

37 Different institutions may use different methods to identify private and professional activities, such as:

- ex-post identification and billing of personal activity: for example, an institution may define a certain amount of data traffic for that institution (based on the institution's average usage in the past) on smartphones provided to employees and invoice users for the excess data traffic; for calls, staff may be asked to identify the private calls to be reimbursed to the institution;
- prior request to the switchboard for personal calls;
- prior request to the switchboard for certain categories of calls (e.g. international calls or calls to mobile phones) and to declare whether the call is professional or personal;
- use of a personal pin code for private calls.

Example 2: *Reimbursement of costs for private phone calls*

Your institution allows the use of office phones for private calls, provided they are declared using a personal code before dialling. At the end of each month, staff members receive a list of their declared calls (with the last three digits of the called number removed) and are asked to reimburse the cost incurred within a month. These records are kept for six weeks, unless there is a dispute related to reimbursement, in which case they are kept until the dispute is resolved. Staff members are informed about these rules (which are laid down in a policy) upon joining the institution.

3.3. Authorised Use of eCommunications Services

38 Your institution may adopt rules or a policy on the authorised use of eCommunication resources in the workplace. This policy can cover issues such as internet access and the use of office phones for private purposes, the monitoring of internet access and prohibited sites.

3.3.1. Transparency and Procedures

39 Staff have to be informed over whether your institution allows the private use of the eCommunications services it provides. As a minimum, this information should be communicated via your policy on authorised use.

R7: **Adopt a progressive approach towards monitoring the authorised use of eCommunications Services**

40 The monitoring of authorised use should be justified and follow a progressive approach. In the absence of suspicious activity, no monitoring of individuals should be carried out. In line with this approach, eCommunications should first be monitored on an aggregate, no name basis. Where it is necessary for your organisation to monitor individual patterns, the identity of individual users should first be masked and accessed only if necessary.

41 If irregular patterns or situations are detected (in terms of volume, size or other indicators of activity), your institution can progressively increase the monitoring. For example, a warning could first be sent to the department(s) concerned that the inappropriate use of eCommunication resources has been detected and needs to be halted. If the inappropriate use stops as a result of this warning, there would be no need to monitor individuals. If it persists, the monitoring can be stepped up.

42 The identification of the user should take place only where there is a concrete suspicion of misconduct (such as inappropriate use of eCommunications resources) and in a defined procedure or in the context of an administrative investigation (see example 3). The suspicion must not be general but reasonable, specific and supported by concrete initial evidence. Your data protection officer should be informed about any case(s) where your institution intends to activate individual monitoring. In such cases, the person(s) concerned should be informed as soon as possible, unless a restriction laid down by Union law or in internal rules under Article 25 of the Regulation applies (see section 3.6 below on administrative enquiries as well as the EDPS Guidance on Article 25).

43 The decision to carry out individual monitoring is a grave one and as such the evidence giving rise to the suspicion of misconduct, the need for individual monitoring, the limits of the investigation and the proportionality of the means used must all be assessed and documented. The decision to monitor a member of staff should be taken by the competent authority responsible for the procedure or the investigation, at the appropriate administrative level, according to a written and publically available policy of your institution on the use of eCommunication resources.

44 Your institution must be able to trace all the steps leading to a monitoring operation and an audit trail of all related processes should be kept. If the EDPS (or other body) questions the necessity of the monitoring, clear audit trails and documented assessments of the measures to be carried out will be what the EDPS (or other body) will be looking for in the investigation.

3.3.2. Internet Access

45 Your institution may want to draw up lists of *prohibited* websites or addresses to which access is blocked, such as sites known or suspected of distributing malware. Similarly, it may want to block websites that will be of no legitimate professional use, such as

gambling or pornography. When trying to access such sites, users should be informed that the site is blocked and why (i.e. which category it belongs to - it is not necessary to proactively publish the list of blocked sites internally).

46 In principle, the source addresses of those person(s) who attempted to access blocked sites should not be logged; target addresses (of prohibited sites) on the other hand may be logged. As a rule, the logging of source addresses for the purpose of verifying authorised use should not be done unless there is concrete evidence of security issues, such as a sharp spike in attempted connections to a blocked site, in line with the data quality principle (see Annex 1).

3.3.3. Telephone use

47 Your institution may want to monitor the authorised use of office or mobile phones in order to verify whether personal use is excessive, or if staff fraudulently fail to declare personal calls.

48 There are a number of equally valid ways of declaring private use. Ex-post declarations of private calls or the use of a pin code for private calls are examples for office phones (see paragraph 37 above).

49 Your organisation's monitoring of suspected irregularities in the declaration of private calls must be based on objective criteria. In principle, the institution should not perform general, systematic or random checks of invoices. The verification should be limited only to invoices exceeding a pre-defined limit, which when compared to the average consumption per employee and the specific tasks performed, may be considered excessive. Such a limit should be identified and clearly stated in your policy.

Example 3: *Policy on the private use of mobile phones for professional purposes*

Your institution provides mobile phones to some members of staff for professional use that they may also use sparingly for private calls.

The policy highlighted to members of staff who request a professional phone outlines that limited, personal use is permitted and special care must be taken over roaming charges when outside the EU. The policy also outlines the ceiling for an average monthly bill; if this ceiling is exceeded, the user will be informed immediately by text message (generated by the system) and may be asked to declare the private calls and to reimburse those above the ceiling. If the ceiling is exceeded three months in a row, the staff member's line manager may be informed.

50 If the ceiling has been exceeded, the member of staff should be allowed to provide an explanation before any action is taken. At this stage, management should not yet have access to the itemised invoice. If the explanations are not convincing, and a reasonable suspicion of misuse still exists, an administrative inquiry can be launched.

51 In this event, the employee should be informed immediately of the administrative inquiry, unless an exception based on Article 25 of the Regulation applies. In the

verification phase, you may ask the employee to justify specific private calls on the invoice that are cause for concern.

3.4. Recording of Dedicated Telephone Lines

52 Your institution may want to record incoming calls to certain phone numbers, such as emergency or whistleblowing hotlines. The recordings may be needed for a particular purpose(s) such as to verify the content of a message in order for the helpline staff to be able to reply appropriately,.

> ***Example 4:*** *Recording of emergency lines*
>
> *Your institution has a dedicated emergency telephone hotline. Calls to this line are recorded. The member of staff in charge of the call is able to re-listen to the message and store it as evidence of operational activities.*
>
> *This may be necessary in order to clarify the content of the message, to provide evidence when following-up judicial or administrative actions, or to help with staff training. Procedures are defined in a document approved by your Director; posters can be found around the institution telling staff about the availability of the hotline and that calls will be recorded.*

53 In line with the principle of proportionality, EU institutions must not record *all* incoming or outgoing calls by the switchboard or specific departments. Only in exceptional circumstances can the general recording of calls received by an entire department (rather than a specific telephone line) be considered necessary. In any case, your institution has to be able to show why the recording of these calls is *necessary* for fulfilling its tasks (including operations). For more information, see EDPS cases 2005-0376 and 2006-0102, available on our website.

> R8: **Adopt internal rules detailing how and why phone calls need to be recorded**

54 Details of the recording (which telephone lines, the conservation periods, purposes for which recordings can be further used and so on) have to be defined in administrative measures adopted at the appropriate level where there is no specific legal basis in Union law.

55 However, it is not enough to state that the recording is *necessary* for your organisation to *carry out its tasks* and/or for its *management and functioning* (Article 5(1)(a) and recital 22, second sentence of Regulation) to justify the recording of calls. You have to document the specific reasons for recording (e.g. in the internal part of the Article 31 record of this processing operation). This documentation should cover why the recording of these specific lines is necessary; possible reasons include the sensitivity of the service provided, its highly technical nature, the volatility of the information exchanged, the potential need to access it in the future and a high likelihood of litigation.

56 If the recording is not continuous, but only activated under specific circumstances, such as when there is a raised security alert, then the documentation also has to detail the procedure for deciding when to activate the recording.

R9: **Inform both callers and staff about the (possible) recording of phone calls *before* it happens**

57 Callers must be informed in advance that their call might be recorded. The best way to do this is via a pre-recorded audio message before an operator takes the call (for lines which are time critical - such as emergency lines - other ways can be considered). This notice should also be highlighted beside the phone number in any telephone directories, such as on your institution's website. Similarly, staff working on the recorded lines must be informed as well. This can be done for example by placing a data protection notice next to the phone itself and/or in the instructions upon taking up the post.

58 A voicemail or message on an answering machine can be considered as consent to follow-up the message left. However, it is not consent for any processing beyond this.

59 Whistleblowing hotlines are one of the most sensitive categories of recorded telephone lines. As they concern allegations of criminal activity or other serious misconduct, whistleblowing lines should be introduced with caution, where there is sufficient evidence to demonstrate necessity. For more information please see Article 29 Working Party Opinion 01/2006 and the EDPS' whistleblowing guidelines.

3.5. Access to Emails in the Absence of the Employee

60 Your institution may want to access the content of absent employees' mailboxes for business continuity reasons. This could for example concern employees on long-term leave, employees who have left the institution or deceased employees.

61 As limited private use is usually authorised, such access constitutes a, possibly justified, interference with their right to privacy.

R10: **Take precautionary measures to reduce the need for accessing personal mailboxes for business continuity purposes**

62 In order to minimise the need to access personal mailboxes in the absence of employees, you have to ensure that relevant emails are also accessible elsewhere. Examples include:

a. instructing employees to save all relevant emails in electronic case files such as in document or case management systems or to archive correspondence in paper files;

b. introducing functional mailboxes for specific units/services/sectors that are accessible to all relevant employees. Recipients could then be asked to copy all business related correspondence to these mailboxes;

c. instructing employees who are leaving the institution to provide complete handover notes.

63 These measures can help to reduce the need to access personal mailboxes. However, access to a personal mailbox may still be needed.

R11: **Adopt a policy on accessing the mailboxes of absent staff if there is a business need**

64 The process for accessing staff mailboxes in their absence should be defined in a policy. This policy can be part of your organisation's more general rules and can also cover access to paper files.

65 Staff must be informed about this policy both in general such as when they join your institution, perhaps via the email use policy, and in specific cases when your institution plans to access their email accounts. The user should be given a detailed explanation for this access, outlining necessity, urgency, the nature and scope of the information sought. As part of the information to be provided to the member of staff under Article 16 , users also have to be informed about their right to object under Article 23 of the Regulation.

66 Where contacting the person(s) is impossible or requires a disproportionate effort, they do not have to be informed (Article 16(5)(b)).

67 If, in spite of the mitigating measures suggested in paragraph 62, access is still necessary, your institution may access the mailbox in line with your policy.

68 However, access to emails may only take place under certain conditions and safeguards. Your institution's email policy must establish clear rules to allow it to access emails in such cases. Access should be incremental, for example, by searching for specific keywords and subject lines before accessing the content of messages, informing the data protection officer and keeping logs to be able to verify the lawfulness of access.

Example 5: *Accessing a mailbox after a member of staff has left the organisation*

According to your institution's rules, staff members have to store all relevant correspondence in a document management system. This includes internal emails to and from line managers approving documents and any other information that future case handlers will require. Combined with handover notes, this makes it unlikely that access to the former employee's mailbox will be required for business continuity purposes.
If such access is still necessary, the former staff member will be informed where possible. In order to avoid that private content is accessed, staff members are instructed to save private correspondence in a folder labelled accordingly, so that it can easily be avoided. According to your institution's rules, their mailboxes are be deleted two months after their departure.

69 Consent is not an appropriate ground for lawfulness to access mailboxes in the scenario covered above. The reason for accessing an email account is for business continuity and because it has been deemed necessary and proportionate. See Article 29 Working Party Guidelines on consent under GDPR, p. 7, for more information.

70 Where access may need to be given to family members of seriously ill members of staff to protect the vital interests of the staff member in question, access may be given with the appropriate safeguards in place.

3.6. Administrative Enquiries and Disciplinary Proceedings

3.6.1. Access to eCommunications data

71 eCommunications data may constitute valuable evidence in administrative enquiries and disciplinary proceedings such as emails showing breaches of confidentiality, internet access logs suggesting dereliction of duties etc.

72 This section concerns internal investigations in the EU institutions under the Staff Regulations; the situation may be different for other investigation activities based on different parts of EU law, such as investigations by the European Commission's DG Competition.

73 The broader data protection implications of administrative investigations and disciplinary proceedings are explored in the EDPS Guidelines of 23 April 2010 on the processing of personal data in administrative inquiries and disciplinary proceedings.

74 In this section, the controller is the entity in charge of the investigation (e.g. IDOC for the European Commission) and not to the controller of the eCommunications system from which the information is obtained (e.g. DG DIGIT for the European Commission).

75 Individual analysis of eCommunications should be carried out only when there is a *reasonable suspicion* of misuse. The facts which give rise to suspicion do not need to be of the same level of concreteness as those that would justify a conviction or bringing a charge. However, a reasonable suspicion should be based on facts or information which would satisfy an objective observer that the person concerned might have committed an offence (see ECtHR, Murray v. United Kingdom (14310/88) judgment of 28 October 1994, paragraphs 55-63).

R12: **Make sure that access to eCommunications data is covered under the rules for administrative enquiries and disciplinary proceedings**

76 How and when investigators can have access to eCommunications data has to be defined in your institution's internal rules for administrative enquiries and disciplinary proceedings.

77 Access to eCommunications must be necessary and proportionate with regard to the purpose of the investigation. The entity (such as IDOC) in charge of the investigation should conduct a concrete assessment of necessity and proportionality, precisely defining the suspected offence and the extent –personal, material and temporal– of the search to be conducted. This assessment should be duly documented before the investigation in order to allow judicial or administrative review in case it is contested.

3.6.2. Covert monitoring

78 In certain circumstances, your institution may want to use covert monitoring, such as keeping detailed logs of all activities of a specific member of staff without telling her in order to obtain evidence of criminal behaviour.

R13: **Provide adequate safeguards when planning covert monitoring, including internal rules under Article 25 of the Regulation.**

79 Keep in mind the following points:

- Covert monitoring is needed to investigate a serious criminal offence in a legal or authorised investigation by EU member state police, other competent law enforcement agents or by the relevant EU investigation bodies;
- the use of covert monitoring is in accordance with the law and has been formally authorised by (i) a judge or other official having the powers to do so according to the laws of the EU member state which requested the use of covert monitoring within your institution, or by (ii) the competent senior decision-making body (such as the Executive Committee or Board) of your institution according to the written and publicly accessible policy of your institution relating to the use of covert monitoring;
- keep a register of all such authorisations and instances of covert monitoring; keep this register available for review by your data protection officer and the EDPS upon request;
- the monitoring is targeted in terms of its material, personal and temporal scope; and provided that:
    a. there are no alternatives to the use of covert monitoring to successfully investigate the case; and
    b. the benefits derived would outweigh the violation of privacy of the individuals observed.
- Covert monitoring requires the use of restrictions under Article 25 of the Regulation together with your institution's internal rules.

3.6.3. Forensic imaging of the content of computers or other devices

80 Computer forensics refers to a number of techniques for inspecting computer systems and their contents with a view to collecting, analysing and presenting electronic evidence to the courts which is legally sound and whose validity and integrity can be trusted. Computer forensic techniques also allow for the retrieval of information that is hidden, lost, damaged or deleted (accidentally or intentionally) that may be relevant in investigations.

81 In most cases, computer forensics will be carried out during an investigation by bodies such as the European Anti-Fraud Office (OLAF) or by national competent authorities in criminal investigations. Therefore, for most institutions, the question of if and how to conduct computer forensics is largely hypothetical. For the sake of completeness, and because some aspects of computer forensics are related to these eCommunication Guidelines, they are addressed here.

82 As computer forensics are invasive, they should be used as a last resort. For the same reason, there must be a solid legal basis (EU Treaties or a legal act adopted as their basis) for their deployment.

83 In some cases, investigators may need to take an entire forensic image of the target device (such as telephones, PCs, laptops and other mobile devices etc.) rather than specific emails or documents. A forensic image may be necessary to preserve the integrity of the evidence collected. Furthermore, depending on the circumstances, investigators may need to perform complex searches and verifications on the materials seized, which cannot be done on the spot. Whether this need exists depends ultimately on the particular facts of each case.

84 The acquisition of the entire contents of a target device is by its nature privacy-invasive. Therefore, as an investigation tool it must be used only where strictly necessary. Investigators should not systematically have recourse to forensic imaging. Specific safeguards should be established to protect the individuals concerned from the risk of abuse. In particular, the following requirements must be fulfilled in addition to the general ones examined in section 3.6.2 above:

- the investigating entity should carry out a necessity and proportionality assessment before launching the investigation and duly document it (similar to paragraph 77). In particular, it should be able to prove that the image is necessary, i.e. that another method would not successfully establish the facts or would be considerably more difficult;
- images or copies of computers should only be taken where there is a concrete suspicion of a sufficiently serious breach, which is corroborated by concrete initial evidence;
- forensic images should not be acquired in cases of minor offences where the amount of information to be collected is minimal nor in cases of low value claims or in cases where the potential benefits of the investigation do not outweigh the potential invasion of private life;
- the content of the copied device should be analysed in a targeted manner. Automated processes and searches, for example, by keywords, should be used to identify the case relevant data, which is to be extracted and placed in the investigation file. Every action must result in a traceable audit trail;
- the individual concerned should have the opportunity, upon request, to be present when the contents are being copied (in certain cases, it may be possible to use restrictions under Article 25 in order to safeguard the investigation - see Guidance on Article 25), or to examine the log files of the operations carried out on the data;
- they also have to be informed about their right to object.

ANNEX: SUMMARY OF DATA PROTECTION PRINCIPLES

The list below gives an overview of generally recognised data protection principles. You will be able to find all or most of them in the data protection rules applicable in the EU. It is for you as a controller to follow them and to be able to demonstrate that. They do not replace the advice given in these guidelines, but provide the philosophy behind them.

1. **Personal data shall be processed fairly, lawfully and transparently.**
   You need to make sure that you have a lawful reason for processing personal data. In many cases, the reason will be that the processing is necessary for the performance of the tasks of your institution attributed to it by law (including necessary internal administrative activities). Consent is another possible reason. Fair and transparent processing means telling people about what will happen with their data and sticking to what you told them.
2. **Personal data shall be processed only for specified explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.**
   Explicitly determine why and how you process personal data. Do not use them in a way that is incompatible with the initial reasons for collecting them (i.e. the initial purpose).
3. **Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data quality').**
   Think about which data you need to achieve your determined purposes and only process those data categories, not more.
4. **Personal data shall be accurate and, where necessary, kept up to date.**
   Make sure that the data you process are accurate. The processing of inaccurate data can result in the wrong decisions being made. Where relevant, make sure that the data are up-to-date.
5. **Grant the rights to access and rectification**
   Persons have the right to access their personal data processed by your institution and to have incorrect data rectified. Make sure that it is easy for them to exercise these rights. This can also help you to make sure that the data are correct and up-to-date.
6. **Personal data processed shall not be kept for longer than is necessary.**
   Carefully consider how long you need to keep the data and then keep for them for that duration, but not longer.
7. **Keep personal data safe**
   Carry out a risk assessment and implement the appropriate state-of-the-art security measures, taking into account the risks of the processing and the cost of implementation.
8. **Rules on transfers**
   Make sure you follow the specific rules for transferring personal data to third parties, especially when transferring outside the EU/EEA.