EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on personal data and electronic communications in the EU institutions

EDPS

Executive Summary

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

Indeed today, eCommunications are essential for the majority of 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 No 45/2001 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 these guidelines 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 data protection Directive (EC) 95/46, which is implemented into the national laws of EU Member States, as well as to the national rules in Iceland, Liechtenstein and Norway.

Summary of Recommendations

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

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.

On billing and budget management:
R4: Instruct external providers to minimise the amount of personal data provided to the institutions for billing purposes wherever possible
R5: Define conservation periods based on the periods for contesting invoices

On authorised use of eCommunications services:
R6: Adopt a progressive approach towards monitoring the authorised use of eCommunications Services.

On the recording of dedicated phone line:
R7: Adopt an administrative measure detailing how and why phone calls need to be recorded
R8: Inform both callers and staff about the (possible) recording of phone calls *before* it happens.

On access to e-mails in the absence of the employee:
R9: Take precautionary measures to reduce the need for accessing personal mailboxes for business continuity purposes
R10: Adopt a policy on accessing staff mailboxes in the absence of staff members.

On administrative enquiries and disciplinary proceedings
R11: Make sure that access to eCommunications data is covered under the rules for administrative inquiries and disciplinary proceedings
R12: Provide adequate safeguards when planning covert surveillance.

Horizontal recommendations applying to all processing operations:
R13: For each operation in which personal data is to be processed, make sure that the purposes are specific, explicit and legitimate
R14: Only collect and process the data you need to achieve your stated purpose(s)
R15: For each processing operation, define how long you will store the personal data
R16: For each processing operation, make sure that data are processed for the stated purpose and not further processed for purposes incompatible with the original one
R17: Inform the persons concerned about how their data will be processed
R18: Provide easy ways for individuals to exercise their rights to access and rectification
R19: Manage your institution's policies on processing eCommunications data
R20: Notify the data protection officer of your processing operations
R21: Keep your documentation and notifications up-to-date
R22: Have a properly documented risk management process in place to secure information
R23: Include data protection clauses in contracts with external service providers
R24: Monitor contractors to ensure they correctly implement the data protection clauses in their contracts.

TABLE OF CONTENTS

1.   INTRODUCTION

1   These guidelines are intended to provide practical advice and instruction to the EU institutions and bodies 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 the Regulation.

2   These guidelines build on previous EDPS decisions and Opinions (on administrative consultations, prior checks and complaints), as well as on the work done by the Article 29 Working Party (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 Article 29 Working Party's interpretation of them wherever appropriate and relevant). Where we do not take a position, the EDPS assumes the one defined in these other documents.

3   These guidelines have been developed on the basis of long-term experience. They are based on the current legal framework. While changes to the data protection rules for EU institutions are on the horizon, the advice provided here will remain relevant. One change that is expected with these new rules is a greater focus on accountability, a shift that these guidelines already anticipate.

4   By following these guidelines you can be reasonably assured that you comply with Regulation 45/2001 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 a 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 administrative 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.).

1.1. Structure

7   These guidelines are split into two parts: a section with general recommendations about data protection when operating eCommunications; and another section addressing specific concerns with more targeted recommendations. Both sections contain practical examples to illustrate where relevant.

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

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

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

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

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

1.2. Scope

12   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 (understood widely, including 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. for administrative enquiries between persons falling under the Staff Regulation and those that don't), the principles are the same. In the end, 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.

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

- telephony, fixed and mobile;
- e-mail; and
- internet.

14   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).

15   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.

2. RECOMMENDATIONS FOR PROCESSING PERSONAL DATA FOR SPECIFIC REASONS

16   This section covers specific concerns about the processing of personal data in eCommunications usage and contains recommendations to address those. These need to be applied in addition to the general recommendations in section 3 below. The general recommendations are always applicable even when not specifically mentioned.

2.1. 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);
- 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 paragraph 95 onwards on 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 e-mail 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 (Aticle 4(1)d) 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.

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

23   The general principle of **purpose limitation** (see section 3.4 below) restricts the further use of personal data which is incompatible with the original purpose(s). For security logs, this principle is **further strengthened** by Article 6(2) of the Regulation, which states that "personal data collected exclusively for ensuring the security or the control of the processing systems or operation *shall not be used for any other purpose*, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences". Examples of uses for "security and control" include incident management, virus scanning, the analysis of breaches and the generation of statistics on resource utilisation. The use of these logs for the purposes of staff evaluation is not allowed.

24   **E-mail 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 e-mail traffic data (volume, type of attached files, e-mail 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 may be needed in specific cases if justified by the system administrator.

> ***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**.

2.2. Billing and Budget Management

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

27   Data processed for monitoring billing and invoices **have to be limited to what is necessary** (as per the data quality principle, see paragraph 95 onwards). 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).

28   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.

R4: Instruct external providers to minimise the amount of personal data provided to the institutions for billing purposes wherever possible

29   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 e-mail traffic data). It is

for your institution to instruct the provider to restrict the categories of data included in the associated invoices wherever possible.

30   Not all data fields mentioned in 2.1 above are relevant for both billing and budget management. For example, e-mail 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.

> **R5:   Define conservation periods based on the periods for contesting invoices**

31   The period of time you plan to store call records or other logs (the conservation period) for purposes of budget management and billing purposes should not exceed the period that is allowed for contesting bills for communication services (see Article 37 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 recommendation R15).

32   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 people (or roles) directly involved in these areas.

33   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.

34   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.*

2.3. Authorised Use of eCommunications Services

35   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.

2.3.1. Transparency and Procedures

36   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 (see also sections 3.5 and 3.7 below on information and documentation).

> **R6:** **Adopt a progressive approach towards monitoring the authorised use of eCommunications Services**

37   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.

38   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.

39   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 one of the exceptions laid down in Article 20 of the Regulation applies (see section 2.6 below on administrative enquiries).

40   The decision to carry out individual monitoring is grave 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.

41 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 (see also the section on accountability at 3.1 below).

2.3.2. Internet Access

42 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).

43 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. This is in line with the data quality principle (see paragraph 95).

2.3.3. Telephone use

44 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.

45 There are a number of equally valid ways of declaring private use. Ex-post declarations of private calls or entering a code for private calls are examples for office phones (see paragraph 34 above).

46 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 the EU institution's policy.

> ***Example 3:*** *Policy on the private use of mobile phones for professional purposes*
>
> *Your institution provides some members of staff with mobile phones for professional use that may also be used sparingly for private calls.*
> *The policy which is given to members of staff who request a professional phone outlines that limited, personal use is permitted and special care must be taken over roaming. 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 member of staff's line manager may be informed.*

47   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 enquiry can be launched.

48   In this event, the employee should be informed immediately of the administrative enquiry, unless an exception under Article 20 of the Regulation applies (see also paragraph 113 below). In the verification phase, the employee can be asked to justify specific private calls on the invoice which are cause for concern.

2.4. Recording of Dedicated Telephone Lines

49   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, or for use as a training aid.

> ***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.*

50   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.

> **R7:** **Adopt an administrative measure detailing how and why phone calls need to be recorded**

51   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.

52   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(a) and recital 27 of Regulation 45/2001) is, on its own, not enough to justify the recording of calls. Complementary information needs to be documented. 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.

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

> **R8:** **Inform both callers and staff about the (possible) recording of phone calls *before* it happens**

54   Callers must be informed in advance that their call will/might be recorded. The best way to do this is via a pre-recorded audio message before an operator takes the call (for lines for which time is crucial - 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 privacy notice next to the phone itself and/or in the instructions upon taking up the post.

55   A voice-mail 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.

56   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' upcoming whistleblowing guidelines.

2.5. Access to E-mails in the Absence of the Employee

57   Your institution may want to access the content of employees' mailboxes in their absence for business continuity reasons. This could for example concern employees on long-term leave, employees having left the institution, or deceased employees.

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

> **R9:　Take precautionary measures to reduce the need for accessing personal mailboxes for business continuity purposes**

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

　　a.　instructing employees to save all relevant e-mails 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.

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

> **R10:　Adopt a policy if accessing staff mailboxes is required in the event staff members are absent**

61　　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.

62　　Staff must be informed about this policy both in general such as when they join your institution, perhaps via the e-mail use policy, and in specific cases when your institution plans to access their e-mail accounts. The user should be given a detailed explanation for this access, outlining necessity, urgency, the nature and scope of the information sought. In addition to the information to be provided to the member of staff under Article 12 (see paragraph 108), users also have to be informed about their right to object under Article 18 of the Regulation.

63　　Where contacting the person(s) is impossible or requires a disproportionate effort, they do not have to be informed (Article 12(2)).

64　　If, in spite of the mitigating measures suggested in paragraph 59, access is still necessary your institution may access the mailbox in line with your policy.

65　　However, access to e-mails may only take place under certain conditions and safeguards. Your institution's e-mail policy must establish clear rules to allow it to access e-mails 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 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,*

66   Consent is not an appropriate ground for lawfulness in access to mailboxes in the situation covered above. The reason for accessing an e-mail account is for business continuity and because it has been deemed necessary and proportionate. See Article 29 Working Party Opinion 15/2001, p. 13 and Article 29 Working Part Opinion 08/2001, p. 3 for more information.

67   Another situation where access may be needed is the case of giving access to family members of seriously ill staff members; where such access is needed for the protection of the vital interests of the staff member in question, the necessary access may be given with the appropriate safeguards.

2.6. Administrative Enquiries and Disciplinary Proceedings

2.6.1. Access to eCommunications data

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

69   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.

70   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.

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

72   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).

> ### R11: **Make sure that access to eCommunications data is covered under the rules for administrative enquiries and disciplinary proceedings**

73   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.

74   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.

2.6.2.   Covert monitoring

75   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.

76   Proposed covert monitoring procedures must be accompanied by a compelling justification, an impact assessment and must undergo a prior check. This is because such procedures involve the processing of personal data on suspected offences and evaluate the suspected person(s), triggering both Article 27(2)(a) and (b) of the Regulation . In his prior check Opinion, the EDPS may impose, as necessary, specific data protection safeguards.

> ### R12: **Provide adequate safeguards when planning covert monitoring**

77   In principle, the EDPS will issue a favourable prior check Opinion if all of the following conditions are satisfied:

- 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;

- a register is kept of all such authorisations and instances of covert monitoring. This register must be 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.

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

78   Computer forensics can be defined as the technological process 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.

79   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 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.

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

81   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 e-mails 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.

82   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 in exceptional cases, where strictly necessary. Investigators should not have recourse to forensic imaging systematically. 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 2.6.2 above:

- the investigating entity (e.g. OLAF) should carry out a necessity and proportionality assessment before launching the investigation and duly document it (similar to paragraph 74). 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; where there are low value claims or in other cases where the potential benefits of the investigation would 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 an 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 20 in order to safeguard the investigation - see points 113 and 114 below), 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.

3. GENERAL RECOMMENDATIONS FOR PERSONAL INFORMATION AND ECOMMUNICATIONS

3.1. Be Accountable!

83   Accountability means that organisations have to respect their data protection obligations and be able to demonstrate that they do so.

84   Accountability is not a specific to eCommunications data, but applies to all operations that process personal information.

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

86   EU institutions process personal information for numerous reasons; recruitment and procurement activities, staff appraisals, the collection of health data in medical files, the setting up of time management systems, CCTV and visitor access to EU buildings are but a few examples. Therefore, EU institutions are responsible and accountable for complying with the data protection rules laid out in the Regulation.

87   In general, institutions have to be transparent and explicit about how they process the personal data related to eCommunications and the monitoring of eCommunications. They have to document their policies and make sure users are aware of them. The

right to privacy also exists in the workplace and people must be made aware if they are being monitored. Institutions cannot assume that staff will know.

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

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

   a. **Define the purpose:** What do you want to achieve and why?

   b. **Legality:** Are you allowed to do it?

   c. **Purpose limitation and security:** How will you ensure that the personal information is used only for the intended purpose?

   d. **Rights of the individual:** How will you inform the persons concerned and ensure that they can exercise their rights (for example, privacy statements, ad-hoc information, access and rectification, possible restrictions)?

   e. **Documentation and notifications:** How will you document what you do and how will you keep it up to date?

90   The following subsections detail the minimum considerations for each of these questions.

3.2.   Why Do You Need to Process eCommunications Data and How You Will Do It?

> R13: **For each operation in which personal data is to be** processed**, make sure that the purposes are specific, explicit and legitimate**

91   Before processing personal information, you have to **define the purpose** for which you need to process it. The purpose has to be **specific, explicit and legitimate**. This analysis is based on your organisation's business needs and has to be documented in the relevant policies (see section3.7 below).

92   Be **specific** about the purpose(s) so that the persons affected will understand the reasons for processing their data. Clear and concise explanations are necessary. Overly broad descriptions (such as to improve user experience) are not sufficient without further explanation. For further reading, see Article 29 Working Party Opinion 03/2013 on purpose limitation, p. 15-16.

93   **Explicitly** defining the purpose(s) ensures that all those implicated by the processing will be aware of what will (and won't) happen to their data.

94   **Legitimate** purposes are those that are "in accordance with the law". In practice, this means having a proper legal basis (see section3.3 below) and complying with the other data protection requirements (such as specific rules for special categories of

data). For further reading, see Article 29 Working Party Opinion 03/2013 on purpose limitation, p. 19-20.

> **R14:** **Only collect and process the data you need to achieve your stated purpose(s).**

95   Having defined the purpose of the processing and demonstrating the legality, you have to consider the **quality of the data**. The principle of **data minimisation** means that you must only process the data you need to achieve the defined purpose(s). (Article 4(1)(c) of the Regulation: personal data processed shall be "adequate, relevant and not excessive in relation to the purposes").

96   This means that you must define what information is required to achieve the desired purpose(s). If data is not necessary, you must not process it. You must not collect or store personal information simply because it *might* be useful later. Where such information is kept for several purposes, ensure that those involved only have access to the data needed for their role in the processing operations. For example, a member of an IT helpdesk may need access to certain user logs to respond to user requests; she does not need the same access as an auditor or a security officer.

> **R15:** **For each processing operation, define how long you will store the personal data**

97   **Retention periods**: Organisations must often keep personal information on file for certain purposes (HR, legal, and so on). Having defined the purpose and the quality of data you need, you must define how long you will keep it. **Conservation periods** have to be defined according to the maxim "**as long as necessary, as short as possible**", taking into account the purpose(s) of the processing. (Article 4(1)(d) of the Regulation : personal data are to be "kept […] no longer than is necessary for the purposes for which the data were collected or for which they are further processed").

98   Where there are different purposes for keeping the same records, access restrictions should be used accordingly. For example, IT help desk staff will need access to recent log files for troubleshooting, while auditors may need access to older log files; the access to files for managing a service and auditing a service need to be tailored according to the needs of each service.

99   Where only some of the personal data needs to be kept for a longer period, you must delete that which is not necessary (e.g. keeping certain logs for a defined period, while keeping user account information for as long as they are active).

3.3. Is it legal?

100   Processing of personal data must be based on one of the legal grounds laid down in Article 5 of the Regulation.

101   Most processing of eCommunications data is likely to be based on the grounds of **public interest** (Article 5(a)), which includes "the processing of personal data necessary for the management and functioning of those institutions and bodies" (recital 27). Most of the specific legal bases should be contained in your institution's

internal rules defining "management and functioning" while Article 37 of the Regulation contains specific rules for traffic and billing data.

102 **Consent** of the individuals whose personal data is to be processed is another ground for lawfulness (Article 5(d)). However, consent must be freely given, without real or potential prejudice that would arise from not consenting. For more information, see Article 29 Working Party Opinion 15/2011 on consent.

103 In the context of employment, the power imbalance between employer and employee makes it unlikely that consent would be valid as a legal ground. For example, if your institution needs to access an employee's mailbox in her absence, the employee's consent would not be the appropriate ground. Instead, it would be necessary for business continuity in the public interest. Similarly, phone calls to emergency lines may be recorded so that operators can listen to the call again in case it is difficult to understand in real time, in order to despatch the necessary assistance; the caller and the person taking the call may or may not have agreed to the recording.

> ***Example 6:*** *Internal staff directory: necessity v. consent*
>
> *An internal* institutional directory *listing names, job title, email, telephone and office number etc. may be "necessary for the functioning" of an institution (Article 5(a) + recital 27 of the* Regulation (E*). Without such a directory, it would be difficult for an organisation to function smoothly. This necessity is sufficient justification to create such a directory. While the consent of staff is not required, informing them is - see section 3.5 below.*
> *Pictures of staff are not an essential requirement for the directory; they are not a necessary element of the directory for the organisation to keep functioning. In this case, consent is an appropriate ground; you cannot oblige all staff to upload photos of themselves.*

3.4. Personal Data Must Only Be Used For the Intended Purpose

R16: **For each processing operation, make sure that data are processed for the stated purpose and not further processed for purposes incompatible with the original one.**

104 **Purpose limitation** is one of the major principles of data protection. The principle is designed to protect individuals by limiting the use of their personal data to pre-defined purposes, except under strict conditions and with appropriate safeguards. For more information, see Article 29 Working Party Opinion 03/2013 on purpose limitation.

105 In some cases, a **change of purpose** may be permissible, where it is outlined in your internal rules and is not incompatible with the original purpose. Incompatible further use is only possible under the conditions of Article 20 of the Regulation.

> ***Example 7:*** *Purpose limitation & IT logs*
>
> *An EU institution keeps logs of internet connections in order to ensure functionality and security of its systems. One of the tasks of the IT administrator is to monitor that the systems work. To do this, she has to have access to these log files, including the websites visited by staff every day.*
> *The head of a different unit requests that the administrator forward the log files of a particular staff member working under her supervision, as she suspects that she is spending a lot of time on leisure websites and social networks, thus neglecting her work duties.*
> *The purpose of keeping log files is to ensure that the systems run correctly and to detect and react to incidents. They are not intended to help managers keep tabs on their staff. The IT administrator must refuse the request.*
> *Alternatively, if an administrative investigation into the behaviour of that staff member had been launched in accordance with the applicable internal rules and the request came from the investigation panel, the change of purpose may be permitted.*

106 You must take special care to ensure the security of the personal data that is collected, processed and stored. Organisations have to take appropriate technical and organisational measures to secure the data to reflect the risks to the persons concerned. This means, among other things, having an information risk management process in place. For more information, see section 3.8.1 below.

3.5. The Right to Know

> R17: **Inform the persons concerned about how their data will be** processed

107   As a general rule, you must inform individuals about how their data will be used **before** the processing starts.

108   The minimum content of the information to be given is defined in Articles 11 and 12 of the Regulation. Persons concerned have to be informed about:

    a.   who is in responsible for the processing (identity of the controller);

    b.   the purpose of collecting, storing and using the data;

    c.   who will the data be shared with/who will be able to access the data;

    d.   if the data is to be collected from the person concerned: is providing the information mandatory or optional? If it is mandatory, what are the consequences of not providing it?

    e.   if the personal information is not collected directly from the person, where was it taken from: what type of data is to be processed? This is for example the case for logging of activities on IT systems: since the users do not know what is being logged, they have to be told about it. On the other hand, in a selection procedure, it is not necessary to repeat all the categories of data requested in the application form in the privacy statement, as the person knows what she provided, a basic referral to 'the content of the application form' is enough.

f. informing the individual(s) about their rights of access to their data and rectification of it; this should include information on how to access this data for example, by including the contact details of the person they should write to.

g. any other information that is necessary to ensure fair processing, such as:

 i. the legal basis for the processing;

 ii. how long the data is to be kept;

 iii. the right to recourse with the EDPS.

109   You should provide this information to the persons concerned in **concise and easily understandable language**.

110   You should do this via a **privacy statement(s)**, since information in policy documents outlining your institution's approach to the processing of eCommunications data is not written specifically to inform those whose data is to be processed. Simply referring to these policy documents is not very user-friendly for the purposes of informing the persons concerned.

111   The shorter a privacy statement is, the more likely it is to be read. In most cases one page will be enough to convey the information required. "**Layered" notices** with a short basic summary linking to a full explanation are also an option.

112   **Publishing privacy statements on the institution's intranet is not enough**. You must actively inform the persons concerned. For new staff, including such information in their welcome pack can be a useful way; providing it via pop-up screens during their first log-on to their computers is another.

> *Example 8:*   *Information about the rules for using IT resources*
>
> *An institution provides the standard ICT services to its staff (telephones, mailboxes, internet access on desktop computers, WiFi, etc.); visitors can use guest WiFi access. Staff are informed about the applicable rules upon joining the institution in their welcome pack, which includes a copy of the policy document and concise one-page privacy statements (all of which are also available on the institution's intranet). Whenever the policy is changed, staff members are informed via email containing a summary of the changes. The policy contains rules on how and when the institution can access the mailboxes of staff members in their absence. Additionally, when these targeted procedures are used, the staff members concerned are informed individually. Since only a few of these processing operations are relevant for visitors, they can be informed in a different way; examples include a privacy statement on the information sheet containing the guest WiFi access codes and/or via a redirection to the privacy statement when first connecting to the network.*

113   In some cases, there may be good reasons for not informing someone about the use of their data immediately, for example in the early stages of an administrative enquiry. The data protection Regulation allows this under certain conditions, which are listed

under Article 20. For more information, see the [EDPS Guidelines on the rights of individuals](#), pages 26 onwards.

114   Examples include the prevention and investigation of criminal offences. If an institution wants to use such a restriction, documentation detailing why this is necessary must be kept. In cases where such restrictions are necessary, the implementing rules on data protection in the institution may require the consultation of the [data protection officer](#).

> ***Example 9:***   *Restricting the right of information*
>
> *A member of staff is suspected of spending several hours of the working day visiting gambling websites.*
> *The policy on access to IT resources states that log files for internet access may be used for administrative investigations and disciplinary proceedings.*
> *An administrative enquiry into the staff member's behaviour is launched in accordance with the applicable rules. Informing her immediately would severely hamper the investigation since she is likely to change her behaviour for the duration of it and frustrate the effort to obtain evidence for her dereliction of duty.*
> *Under these circumstances, delaying the information may be justified. The investigator leading the enquiry has to document which of the exceptions under Article 20 of the Regulation applies and why it is necessary to use it. When the restriction becomes unnecessary, the member of staff must be informed.*

3.6. The Rights of Access and Rectification

> R18: **Provide easy ways for individuals to exercise their rights to access and rectification**

115   Individuals (also known as [data subjects](#)) have the **rights to access and rectify personal data relating to them**, according to Articles 13 and 14 of the Regulation. Your institution only needs to give access to the information it has about that person, these rights **do not oblige your institution to keep data it would not have otherwise kept**.

116   The information you have to provide is detailed in the [EDPS Guidelines on the rights of individuals](#), pages 9 onwards. To summarise, you have to provide the following:

    a. Whether the personal information of the requester is being processed;

    b. Details about the processing operation, for instance in a privacy statement plus additional information where relevant;

    c. which information is being processed and who it was obtained from;

    d. the logic of any automated decision-making process. For example, if the bill for your professional mobile phone exceeds 200€, you receive a warning. If the bill exceeds 200€ two months in a row, your line manager will be informed.

117   The legal **time limit to reply** to a request for **access or rectification** under the data protection Regulation is three months; however, the implementing rules on data

protection in your institution may impose stricter deadlines. Check with the data protection officer if you're not sure.

118   If rectification by changing data is not possible (e.g. because of having to preserve the integrity of log files), the person(s) should be able to have their disagreement documented.

119   Exceptions to these rights are limited under Article 20 of the data protection Regulation. For more information, see EDPS Guidelines on the rights of individuals, pages 26 onwards.

Example 10: *Granting access to information*

An institution allows staff members to use office phones for private calls, on the condition that these calls are declared by using a specific code. The fees for these calls are paid for by the relevant staff members.
The application used to collect this information allows staff members to check their own list of declared calls via a link on the intranet of the institution. If the member of staff notes an error, a contact form allows them to alert those responsible to make the necessary corrections.

3.7. Document What You Do

R19: Manage your institution's policies on processing eCommunications data

120   Accountability is about doing the right things responsibly in reproducible ways. Well developed and well managed policies are a key component of accountability.

121   Such policies help institutions to see how to implement the recommendations outlined in these guidelines, such as those on the purpose limitation principle, data quality principles and informing all those whose personal data is to be processed.

122   These policies have to be reviewed regularly and adapted as necessary.

R20: Notify the data protection officer of your processing operations

123   The Regulation contains **specific obligations about documentation**. Under Article 25, all processing operations have to be notified to your data protection officer and she will have a notification form for you to complete. You have to notify her *before* the processing begins, so that she is able to offer advice, suggest improvements and notify the EDPS for prior checking if necessary.

124   In addition, **some risky processing operations** have to be **notified to the EDPS** for prior checking; for eCommunications, this concerns basically the processing of certain special categories of data listed in Article 27(2)(a) of the Regulation and processing intended to evaluate personal aspects relating to the person affected (data subject) (Article 27(2)(b). The most relevant for eCommunications concern the processing of data related to suspected offences, offences or security measures. The reference to security measures here does not refer to information security, but to actions like forced admission into psychiatric treatment - coercive measures taken against a person for her security (or those of others). Other examples include traffic analysis intended

to evaluate staff members or covert surveillance for use in administrative inquiries. The data protection officer will notify the EDPS, but she will have to liaise with the person in charge of the processing for filling in the notification form to be sent to the EDPS. For your own planning purposes, you should take into account the time it will take the EDPS to issue his Opinion (up to 2 months, extendable for a further 2 months, not including time suspended when requesting additional information).

> **Example 11:** *The use of log files in administrative inquiries*
>
> *If your institution updates its internal rules on administrative inquiries to reflect the use of log files in the procedure, the original notification you sent to your data protection officer on administrative inquiries must be updated accordingly. As the use of log files is not a purpose in itself but part of administrative inquiries, a new separate notification is not necessary.*

125 The following are some examples of processing operations that do <u>not</u> have to be notified to the EDPS:

   a. processing of telephone data solely for billing and budget management purposes, provided that there is no intention to verify authorised use or to evaluate employees;

   b. processing of traffic data (e.g. e-mail and internet) for security or traffic management purposes, which is carried out automatically and on a no-name basis, provided that there is no intention to verify authorised use or to evaluate employees.

R21: **Keep your documentation and notifications up-to-date**

126 It is your responsibility to keep your documentation and notifications up to date. Whenever there are changes in your procedures that affect the content of the notification or the privacy statement or are relevant from a data protection perspective, inform your data protection officer. This is an important part of the accountability process.

3.8. Technical and Organisational Security Measures

3.8.1. Manage your information risks

R22: **Have a properly documented risk management process in place to secure information**

127 Your organisation must put the appropriate technical and organisational measures in place to safeguard the secure use (both system and personal data security) of the eCommunication networks and terminal equipment, together with service or network providers if necessary. According to Article 22 of the Regulation, these measures should ensure a level of security appropriate to the risk presented to all information, taking into account any available technical solutions and the cost of their implementation.

128   This means that you have to implement an **information risk management process** according to the established principles of good practice (e.g. ISO/IEC 27000 series). The first step is an assessment of the risks, which should include an analysis of the use of eCommunications resources. This assessment will help you to determine the main security risks and provide the basis for selecting the appropriate controls to be put in place in order to reduce the risks to a level acceptable to management. The risk management process has to include a periodical review of the risk assessment and the appropriateness of the safeguards and controls.

129   You must properly document the information risk management process according to established standards for such procedures and **communicated** as a policy of the institution. It must also be **regularly reviewed** to ensure it remains effective and aligned with new and changing business objectives.

130   The process (especially in the analysis of security risks) should **not only involve those staff that deal with security** in the EU institution. The an**alysis needs to take into account the impact on all areas of the business**, so a variety of representatives (HR, data protection officer, data protection coordinator, core business activities) should also be included in discussions.

131   You should clearly communicate the outcome of the information risk management process and of existing security risks to all those affected or potentially affected; management and others may benefit from more detailed communication.

3.8.2. The outsourcing of services

R23: **Include data protection clauses in contracts with external service providers**

132   EU institutions may want to outsource functions related to the processing of eCommunications data to external providers. For instance, your organisation may rely on external firms to carry out security monitoring, anti-virus management, e-mail management or to compile statistics. In these cases, appropriate precautions have to be taken. In particular:

   a. your institution should exercise great care over choosing a provider which provides sufficient guarantees over the technical and organisational security measures required under the Regulation: the **institution is responsible for ensuring the provider's compliance** with those measures;

   b. the relationship between the EU institution and the provider has to be **formalised in a contract or legal act** binding the processor to the controller. The document has to stipulate that:

      i. the provider shall act **only on instructions** of your organisation;

      ii. the **confidentiality and security obligations** set out in the Regulation shall also be incumbent on the provider (unless similar obligations under national law implementing Directive 95/46/EC already apply to the provider). For contractors outside the EU, adequate safeguards

need to be assured. On the question of transfers of data, see the [EDPS Position Paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies](), especially pages 18-21.

> **R24:** **Monitor contractors to ensure they correctly implement the data protection clauses in their contracts**

133   The [Regulation]() also applies to any service that is outsourced and it is up to the institution to ensure that external companies follow the principles laid out and implement the relevant safeguards. For example, asking for the contractor's staff to sign confidentiality declarations similar to those signed by staff in your own organisation.

ANNEX 1: SUMMARY OF DATA PROTECTION PRINCIPLES

The list below gives a quick overview of generally recognised data protection principles. You will be able to find all or most of them in data protection rules 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 and lawfully.**

   You need to make sure that you have a lawful reason for processing personal data. This could 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). Fair 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 that initial purpose.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.**

   Think about which data you need to achieve your determined purposes and 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 - inaccurate data can lead to taking wrong decisions. 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 in making sure data are correct and up-to-date.

6. **Personal data processed shall not be kept for longer than is necessary.**

   Think about how long you need to keep the data and then keep for them for that duration, but not longer.

7. **Keep personal data safe**

   Do a risk assessment and take appropriate security measures based on the state of the art, 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.