EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on the protection of personal data in IT governance and IT management of EU institutions

23 March 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Regulation (EC) No 45/2001 (the Regulation) sets the legal framework for the protection of individuals with regard to the processing of personal data by EU institutions and bodies, offices and agencies (EU Institutions).

EU institutions rely on information systems and databases to perform a range of operational and administrative tasks. A great part of those information systems process personal data, therefore their full compliance with the Regulation is of utmost importance. Moreover, under the General Data Protection Regulation (GDPR), data protection by design will, for the first time, become a legal obligation. This will mean that data protection and privacy must be built in to the design specifications and architecture of information and communication systems and technologies. Similar obligations will apply to EU Institutions and Bodies.

The purpose of these Guidelines is to give EU institutions practical advice on the processing of personal data through the entire life cycle of an information system in order to ensure compliance with data controllers' legal responsibilities. Nevertheless, EU institutions remain accountable for the adequate processing of personal data according to data protection requirements.

The Guidelines describe the data protection aspects related to the processing of personal data through information systems.

They also present 26 recommendations aimed at helping the EU institutions to improve accountability in relation to the development, operation and maintenance of the information systems and databases they use.

The list of actions and measures recommended in the Guidelines is not intended to be exhaustive or exclusive. EU institutions may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. In this case they will need to demonstrate how these measures lead to an equivalent protection of personal data.

1. INTRODUCTION

1 The purpose of these guidelines is to assist EU institutions and bodies ("EU institutions") in designing and implementing an internal control system[1] for the management and governance of their IT systems[2] in order to ensure that their processes and systems comply with their legal responsibilities regarding the processing of personal data throughout their entire life cycle, as set out in Regulation 45/2001[3] ("the Regulation"). The present guidelines complement EDPS guidelines on specific IT related matters, such as those on mobile devices[4], web services[5], mobile apps[6] and cloud computing[7].

2 As the independent supervisory authority competent for the processing of personal data by the EU institutions, the European Data Protection Supervisor (EDPS) may among other tasks issue Guidelines on specific issues related to the processing of personal data.[8] The present Guidelines are the result of a process where the EU institutions have been consulted.

3 In order to ensure that personal data is processed in line with data protection principles, "data protection by design" and "data protection by default" constitute good practices in the management of IT systems[9].

---

[1] The approach taken in these guidelines is compatible with the European Commission's Revised Internal Control Framework (C(2017) 2373), which structures internal control in five internal control components and 17 principles. Accountability and risk management are central principles in this framework as well as in data protection, While all principles are relevant for governance and management, IT related processes are in particular concerned with internal control principle 11 which concerns control over technology and IT security, and principle 13 which concerns information and document management and in particular compliance with data protection rules.

[2] Throughout the guidelines the terms "information system" and "IT system" are interchangeable.

[3] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8 of 12.1.2001, p. 1.

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

[5] Guidelines on the protection of personal data processed through web services provided by EU institutions, 7 November 2016.

[6] Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions, 7 November 2016.

[7] Guidelines on the protection of personal data processed by cloud services provided to European Union institutions, 16 March 2018.

[8] In the exercise of the powers conferred under Articles 41(2) and 46(d) of the Regulation.

[9] More specific guidance on the principles of data protection by design and by default is expected to be developed by the European Data Protection Board, to which the EDPS will contribute. Furthermore, the EDPS intends to publish an opinion on future policies to develop a more comprehensive concept of Privacy by Design.

4 The establishment of an effective internal control system is the responsibility of the management of an institution. It is good practice for the management to demonstrate its "accountability" by taking full account of its obligations.

5 Following the adoption of the General Data Protection Regulation (GDPR)[10], the principles of accountability, data protection by design and data protection by default will become increasingly important also for EU institutions as the EU legislator has embedded these principles as legal obligations in the GDPR and has declared[11] that the data protection legislation for EU institutions shall be adapted to apply the same principles, ideally at the same time[12].

6 These guidelines cannot provide all necessary guidance for the implementation of data protection by design in specific IT solutions, as concrete technical measures will need to be designed and implemented for each specific technical context. However, introducing accountability for privacy and data protection also in IT management and IT governance processes is a necessary condition to meet these and other obligations in the future.

7 The guidelines should be considered by Data Protection Officers (DPOs) and Data Protection Coordinators or Contacts (DPCs) within each EU institution, as well as IT staff and other services concerned with the development and operation of IT systems, and to all persons carrying responsibility for the EU institutions acting as controllers. They will also be useful to senior management in supporting a culture of data protection from the top of the organization.

8 While the purpose of these guidelines is to make it easier for EU institutions to fulfil their obligations, they do not take away any of the responsibility of the EU institutions applying them. The measures recommended in these guidelines are not intended to be exhaustive or exclusive. They are flexible enough to allow the EU institutions to start the expected process on accountability, and to be future oriented by considering expected legislative changes. EU institutions may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. Their effectiveness will need to be justified in writing.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

[11] Recital 17 of the GDPR.

[12] At the time of publication of these guidelines, the legislative process on the new instrument replacing Regulation 45/2001/EC is not completed. However, it is already clear that it will mirror the relevant provisions of the GDPR for EU bodies. The present version of the guidelines refers to the GDPR where appropriate. After the publication of the new data protection regulation, an updated version with references to it will be provided.

2. SCOPE AND STRUCTURE OF THE GUIDELINES

2.1. Scope

9 The Regulation specifies the obligations of the controllers within EU institutions with regard to the processing of personal data by EU institutions and provides individuals with legally enforceable rights to data protection.

10 The processing of personal data in information systems of EU institutions must fully comply with the Regulation.

11 The guidelines present recommendations to help EU institutions to strengthen their accountability in data protection throughout the entire life cycle of information systems development, including operations and maintenance of existing systems as well as their disposal. They help to establish an internal control system for IT governance and IT management that enables the controller to achieve compliance, to verify it and to demonstrate compliance with its obligations.

12 Measures proposed in the guidelines do not cover technical aspects of developing IT systems for a specific purpose or using a specific technology. The EDPS continues to provide advice on such issues in thematic Guidelines (e.g. on mobile applications, web services, mobile devices, cloud computing).

2.2. Structure of the Guidelines

13 Chapter 1 introduces the purpose of the guidelines.

14 Chapter 2 defines the scope and the structure of the document.

15 Chapter 3 provides general definitions of accountability, IT governance and IT management.

16 Chapter 4 presents the data protection legal framework and gives an overview of generally recognised data protection principles that should be considered throughout the entire life cycle of an information system.

17 Chapter 5 explains how to integrate data protection requirements into the life cycle of an information system[13].

[13] The life cycle of an IT system model used as reference in this document is based on the RUP@EC®- IBM® Rational Unified Process®.

3. KEY CONCEPTS: IT GOVERNANCE, IT MANAGEMENT, ACCOUNTABILITY

3.1. IT governance and IT management

18 The terms "IT governance" and "IT management" refer to central functions in an organisation. These functions have to ensure that the IT environment of the organisation is aligned with its objectives.

19 *IT Governance Institute (ITGI) formed by ISACA*[14] defines IT governance as:

> *IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.*

20 IT governance has a strategic orientation (what to do) while IT management is more tactical (how to do). IT management comprises various processes and functions.

21 For practical implementation of IT management and governance there are some best practices in use such as ITIL[15] (Information Technology Infrastructure Library) for management and COBIT (Control Objectives for IT and related Technology) for governance.

22 According to COBIT[16] there is a clear distinction between governance and management:

> *Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.*
>
> *Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.*

23 With the centralisation of IT functions in several EU institutions, the establishment of appropriate governance structures has become more important, in order to ensure that the needs and concerns of those parts of the organisation which do no longer operate separate de-centralised infrastructures are properly reflected in the governance of the

---

[14] ISACA (Information Systems Audit and Control Association) is a non-profit, independent association that advocates for professionals involved in information security, assurance, risk management and governance. ISACA formed the ITGI to focus on research on IT governance and related topics.

[15] ITIL (Information Technology Infrastructure Library) is a best practice framework for IT service management. It reflects a life cycle of IT service. ITIL gives guidance on approaches, functions, roles and processes. While ISO 20000 is a standard and code of practice. ISO 20000 -1 provides requirements for a service provider to deliver managed services. ISO 20000-2 presents code of practice.

[16] COBIT is the framework for the governance and management of enterprise IT. It is the product of a global task force and development team from ISACA.

general IT infrastructure. As far as IT is concerned, accountability should be a concern of the governance structure and process.

24 IT governance structures and processes must be designed to ensure compliance with data protection principles and their effective implementation. They should also cover organisational and staff related aspects, such as clearly setting roles and responsibilities, raising awareness of all staff on existing data protection law and policies.

25 Roles in data protection at different levels within an EU institution e.g. directorates, units, as well as allocation of responsibilities, should be clearly defined in its IT governance and management structure.

3.2. Accountability in data protection

26 The term "accountability" has been used in a diversity of contexts and has been developed in recent years to describe a comprehensive approach to meeting data protection requirements beyond pure compliance with the letter of the law.

27 The Article 29 Working Party describes in its opinion[17] that accountability's *emphasis is on showing how responsibility is exercised and making this verifiable*.

28 EDPS in its opinion[18] on the data protection reform package states that the principle of accountability lays down a greater emphasis on the responsibility of the controller. As a general rule, the controller must adopt policies and implement appropriate measures to ensure and be able *to demonstrate* compliance with the data protection rules, and to ensure that the effectiveness of the measures is verified.

29 This verification may be done by using internal resources such as compliance functions in an organisation and/or internal audit functions as well as external resources such as organisations providing certifications, codes of conduct, external auditors etc.

30 Article 5 of the GDPR[19] provides for accountability by stipulating that "*the controller shall be responsible for, and be able to demonstrate compliance with the data protection principles of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation' and security ('integrity and confidentiality')*".

31 Accountability depends on the highest level of management of an organisation which has to ensure that the entire organisation responds to its obligations.

---

[17] Opinion of Art. 29 WP 3/2010 on the principle of accountability.

[18] Opinion of EDPS 7/03/2012 on the data protection reform package.

[19] As explained in paragraph 5, the legislator has declared that the data protection legislation for EU institutions shall be adapted to apply the same principles, ideally at the same time.

R1: It is of utmost importance that data protection principles should be unambiguously supported at management level.

32 The management may delegate responsibility for the implementation of its policies on the basis of a clear definition of mandate and powers.

R2: Senior management, whether or not performing the role of the controller for specific data protection operations, has to be accountable for data protection. If not themselves performing the role of the controller, the senior management should still take specific responsibility to ensure compliance with Data Protection rules, e.g. by setting up appropriate organisational structures and procedures, so that operational management is provided with the means and powers to perform the role of controller and ensure compliance effectively.

33 Even though in the Regulation the controller is the sole responsible entity regarding data protection, with the introduction of accountability the Senior Management must give the controller of their institution everything that is needed to control the processing operations in compliance and rectify problems

R3: Senior management should designate a responsible[20] for data protection (e.g. Data Protection Officer, Data Protection Coordinator) and provide the responsible with a mandate to implement data protection policies.

34 The DPO or DPC should not only provide advice to controllers in their domain of responsibility, but must also have the right to obtain information on the processing operations as it is necessary for the performance of their tasks, and to report directly to senior management any observations regarding processing operations of circumstances that might affect the rights of individuals with respect to the processing of their personal data.

35 Guidance by the data protection responsible on the proper application of the organisation's policies must be followed by all staff involved in the relevant processes.

R4: Existing policies and procedures on data protection should be well known by all staff. This can be ensured through e.g. mandatory induction training, provision of informative material or recurrent training.

36 Management cannot rely on the proper implementation of its policies unless their effectiveness is regularly verified.

R5: Policies, procedures as well as responsibilities and functions regarding data protection should be regularly monitored and maintained.

[20] More details on role of Data Protection Officer to be found under the Guidelines on Data Protection Officers ('DPOs') provided by Art 29 Working Party

37 The responsible for IT governance should be aware of possible occurrences of shadow IT[21]. To mitigate this problem the awareness of the staff has to be raised to ensure compliance measures actually cover all (essential) systems. The senior management should be made aware of issues with shadow IT and the associated risks.

3.3. Data protection by Design and by Default

38 Article 25 of the GDPR obliges controllers to "*implement appropriate technical and organisational measures (…), which are designed to implement data protection principles, (…) and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*". The controller shall observe this obligation both "at the time of the determination of the means for processing", i.e. when the processing systems are designed, developed and tested, and *"at the time of the processing itself*," i.e. when the system is running in production mode.

39 It shall further ensure that, "*by default, only personal data which are necessary for each specific purpose of the processing are processed"* (data protection by default).

40 The controller can only comply with these obligations if its IT governance and management as well as systems development processes are organised in such a way that data protection considerations are taken into account at each step.

41 Section 5 explains how these obligations shall be taken into account in each phase of the lifecycle of an IT system and in the corresponding horizontal processes. This begins with the inclusion of high level data protection requirements in the project charter during the inception phase, continues with the definition of functional and non-functional data protection requirements as part of the system requirements and the integration of appropriate safeguards and measures in the design, their verification during the tests, inclusion of appropriate steps, such as notifications and monitoring in the operational procedures and the appropriate training of users and other relevant staff when the system becomes productive. In the procurement of IT systems and services, EU Institutions as other public sector entities are expected to integrate data protection elements in their tender specifications[22], in order to encourage the manufacturers and providers of

[21] The term "shadow IT" refers to IT systems which are not under the responsibility of the organisation's main IT function, but managed and governed by another operational or administrative function for their own purposes. This separate organisation often makes it more difficult to ensure compliance with the rules of the organisation. Also IT systems used by employees with or without formal permission by the organisation are considered "shadow IT". This includes in particular mobile devices in a BYOD context, for which the EDPS guidelines for mobile devices provide recommendations.

[22] When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers

products and services to take account of data protection by design in their development processes. Such encouragement shall contribute to advancing the state of the art in data protection by design.

42 For EU Institutions, data protection by default is particularly relevant for systems which directly interact with users, inside or outside the EU Institutions. Where appropriate, any processing operations shall be limited to what is the absolutely necessary, as regards "*the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*[23]" for persons or organisations. This should also be applied to any tracking functions, e.g. in the context of web services or mobile apps-

and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

[23] GDPR, Article 25(2).

4. LEGAL FRAMEWORK FOR DATA PROTECTION

43 This section provides a brief overview of core concepts of data protection which should be taken into account in all IT management and governance processes.

44 In addition to the Regulation, these Guidelines consider also concepts of the GDPR which will become mandatory for EU institutions when the Regulation will be adapted to the GDPR. These concepts complement and reinforce the principles laid down in the Regulation and are in full compliance with the current framework. They are already considered good practices and can be applied in the present legal framework.

Personal data

45 According to Article 2 of the Regulation, personal data shall mean any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.[24]

Data subject

46 The data subject is the person whose personal data are collected, held or processed.

Controller

47 The controller is the institution or body that determines the purposes and means of the processing of personal data. In particular, the controller has the duties of ensuring the quality of data and of notifying the processing operation to the data protection officer (DPO). In addition, the data controller is also responsible for the security measures protecting the data.

Processor

48 A processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Legal basis for the processing of personal data

49 Article 5 of the Regulation sets out the legal basis for allowing the processing of personal data, namely;

1. processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties,
2. processing is necessary for compliance with a legal obligation to which the controller is subject,

[24] For more information and examples see the EDPS Glossary on Personal Data and the Art 29 WP Opinion 04/2007 on the concept of personal data.

3. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
4. the data subject has unambiguously given his or her consent,
5. processing is necessary in order to protect the vital interests of the data subject.

4.1. Data protection requirements

50 The list below gives a quick overview of generally recognised data protection principles.

51 These principles have formed the backbone of data protection since its inception and they are incorporated in the Regulation. They are presented here according to the model found in Article 5 of the GDPR.

1. **Lawfulness, fairness and transparency**[25]

- Keep transparency on processing of data vis-a-vis data subjects;
- Inform data subjects about the processing, e.g. its purpose and the identity of the controller;
- Communicate clearly to data subjects how, to which extend and for which purpose their personal data will be processed;
- Make sure that a clear legal basis exists for the processing of personal data and that processing does not exceed the limits of this legal base;
- If consent forms the legal basis, the consent needs to be bound to a purpose, registered and a possibility to withdraw consent has to be given;[26]
- Respect the rights of individuals to access and rectify their data;
- Develop procedures and instructions that clearly explain how data subjects can exercise their right to access and to rectify their data in each phase of data processing;
- Implement functions in the IT system to respond to access, modification or blocking requests and to objections to processing;
- Adopt internal rules to review the validity of the legal basis in case of a change, e.g. the withdrawing of consent.[27]

2. **Purpose limitation**

- Process personal data only for specified explicit and legitimate and limited purposes;
- Limit processing of data through an IT system to its primarily specified purpose;

[25] See also section 5.6.1 on Information to data subjects and transparency.

[26] See also the EDPS Glossary on Consent.

[27] See also the EDPS Glossary on Consent.

- Ensure purpose limitation if different kinds of data are collected and processed for different purposes;
- Adopt internal rules for the assessment of compatibility needs on a case-by-case basis[28] to allow a change of purpose;
- Communicate clearly to data subjects any change of the primarily specified purpose of processing their personal data.

3. Data minimisation

- Ensure that personal data is adequate, relevant and not excessive for the purpose;
- Limit categories of personal data chosen for processing to a data collection that is directly relevant for the originally specified purposes;
- Consider and make use, if feasible, of special privacy enhancing technologies that allow for avoiding excessive use of personal data or enabling the use of anonymised data.

4. Accuracy

- Ensure that personal data is accurate and up to date;
- Implement processes to ensure and maintain accuracy of processed data, e.g. by automatically checking the quality of information keyed into the system before processing;
- Ensure that the data subject has the possibility to rectify data that is no longer accurate.

5. Storage limitation

- Keep personal data no longer than necessary for the originally specified purpose;
- Determine upfront retention time for data kept in a form which permits identification of data subjects;
- Ensure that required retention periods are proportionate to the purposes of data collection and limited in time. Assign and manage separately retention time related to data collected for different purposes.
- Special caution has to be taken if personal data is stored on paper due to its existence being hard to trace;
- Design IT system features to allow to manage the retention time and perform the necessary subsequent actions: deletion or anonymisation.

[28] Art 29 WP Opinion 03/2013 on purpose limitation.

6. Integrity and confidentiality

- Ensure that personal data is secure;
- Perform a security risk assessment and plan for mitigation measures;[29]
- Be aware that a paper copy can circumvent other mitigation measures set for the IT system, e.g. Access Control Lists.
- Based on the risk assessment, design and implement organisational and technical measures to mitigate risks to a level that is acceptable, avoid processing operations for which mitigation would not be effective, and ensure that a clear decision is made by the responsible management of which risks are accepted and why. As data protection risks are related to the fundamental rights of others, externalisation of risks (insurance) is a less viable option than in other domains of risks.

7. Accountability

- Make sure that compliance with the principles above can be demonstrated.

52 Further to these principles, controllers are obliged to respect the rights of data subjects to access, rectification, erasure, restriction of processing, object to processing in particular with regard to automated decision making.

53 The controller has to observe its obligation to only transfer personal data to entities in third countries if an adequate[30] level of protection is ensured.[31]

[29] See for instance the EDPS guidelines on Security Measures for Personal Data Processing.

[30] See the EDPS Position paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies.

[31] See also Annex 1 on the Processing by external organisations and transfers of personal data.

5. DATA PROTECTION REQUIREMENTS IN THE IT SYSTEM DEVELOPMENT LIFE CYCLE

54 This chapter describes processing of personal data throughout the life cycle of an IT system[32], from development through operations and maintenance of IT systems, as well as horizontal processes such as project management.

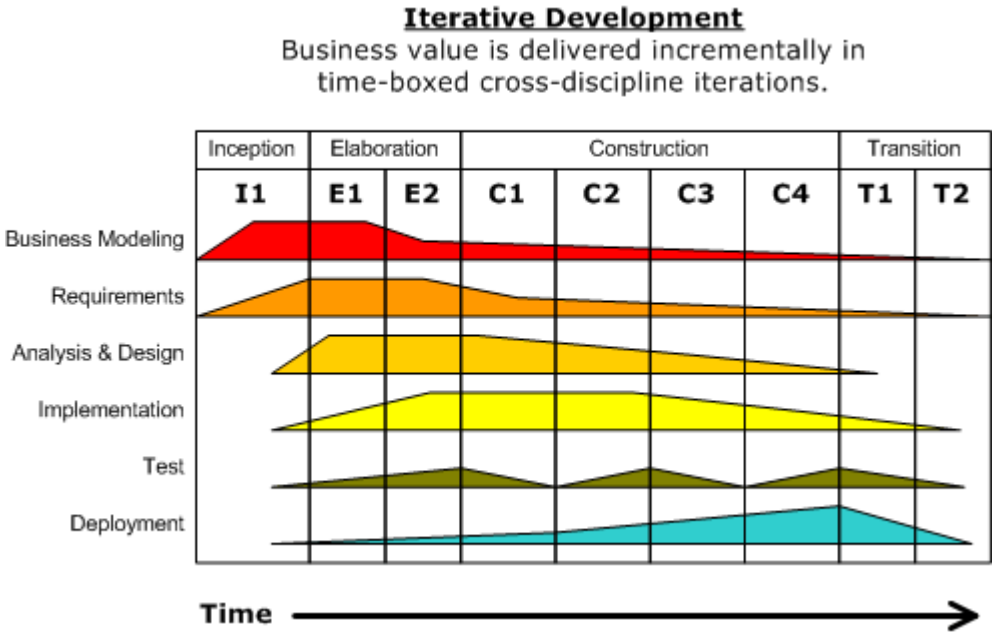

Figure 1: Life cycle phases (source: Dutchguilder, public domain**)**

55 The table attached in Annex 2 presents relevant recommendations considering data protection requirements (see the following sections) in the different phases of the life cycle of an IT system.

5.1. Inception (Start)

56 The inception phase is about setting up the scope of the project and getting agreement on the high level requirements of the project.

57 The responsible for data protection (e.g. Data Protection Officer, Data Protection Coordinator DPO/DPC) should be considered as a stakeholder of an IT project and among others might help to facilitate the protection of any personal data processed by the respective IT system as an end-product of the project. The DPO/DPC should be involved from the inception phase of the project.

R6: As a starting point, it should be determined whether data processed via the respective IT system is personal data or not, or whether it can become personal data as the result of such processing.

[32] The life cycle of an IT system used as reference here is based on the RUP@EC®- IBM® Rational Unified Process®; development methodology tailored for European Commission.

58 If the processing of personal data is foreseen, the legal basis of the processing should be determined.

59 The data protection risks and applicable safeguards should be identified at high level.

R7: High level data protection requirements should be included in a project charter as this document contains the scope statement and high level requirements and is an outcome of the inception phase.

60 At this stage, the high level risks[33] that might affect the processing of personal data should be taken into account. In the light of the upcoming revision of the legal obligations it is recommended to perform a so called Data Protection Impact Assessment (DPIA) in accordance with the GDPR.

61 A risk management process should be conducted during the course of the whole project life cycle[34].

5.2. Elaboration (Plan)

62 The elaboration phase determines the work that takes place in the following project phases. In these phases a future IT system will be designed based on requirements to be collected.

5.2.1. Requirements collection

R8: Data protection requirements should be collected from stakeholders and documented in the IT system's specification phase.

63 The requirements should be maintained and reviewed following the usual project lifecycle methodology. The responsible for data protection (e.g. Data Protection Officer, Data Protection Coordinator) should be consulted by the project manager so that the DPO/DPC can provide the project manager with a comprehensive overview on data protection requirements.

64 Data protection is reflected in functional and non-functional requirements[35]. Functional requirements include in particular the capabilities needed to ensure data subject rights, such as access (GDPR Art. 15), data portability (GDPR Art. 18), rectification (GDPR Art. 16), erasure (GDPR Art. 17), as well as functions to ensure the limitation of retention time (GDPR Art. 5 e). Non-functional requirements include the observation of the principles of data minimisation and purpose limitation (GDPR Art. 5 b and c),

[33] In the EDPS Guidance on Security Measures for Personal Data Processing a risk is defined as "effect of uncertainty on objectives". High level risks are identified at the inception phase. The full risk assessment is conducted in the planning phase and maintained through the whole project life cycle.

[34] Ditto.

[35] Non-functional requirements are also considered quality requirements according to ISO 25010.

which need to be take into account when designing data structures of a system, as well as broader objectives such as security and auditability.

65 The integration of data protection requirements in this phase is the precondition for the appropriate decisions to be taken in the design phase.

5.2.2. Design

66 The design phase establishes how requirements will actually be implemented in the system. It defines the system's building blocks and functionalities and their interaction. In this phase e.g. security measures will be defined that are needed to protect personal data being processed.

67 It is important for technical staff of an IT project as well as for the data protection experts to be up-to-date with the latest developments in existing technologies and products enabling and implementing data protection requirements.

68 With the new data protection framework, 'data protection by design' and privacy-enhanced technologies will become mandatory tools for a better protection[36]. While all functional and non-functional data protection requirements must be considered in the design process, also the design decisions must take account of the data protection features of the chosen technological approaches. Modules and functions for re-use should be chosen so that they do not perform processing operations, including the collection of data which are not necessary for the purpose of the system-For example, designers should not revert to function libraries that have been developed with the objective to collect as much data as possible or to take detailed records of user actions which might in other contexts be used for profiling purposes. Designers should also avoid using tools which communicate personal data to third parties. Where technologies are available that contribute to improved data protection, these should be given preference over less privacy enhanced ones. This approach will help to develop IT systems sufficiently flexible to ensure appropriate protection of personal data.

69 Where the amount of processing may be determined by the data subject, the initialisation values for the relevant parameters shall be set so that the most limited processing operations take place, with the users' possibility to choose more comprehensive processing operations, having a real choice.

70 Article 22(2) of the Regulation lists a set of security objectives and generic risks that must be mitigated. The controller shall implement measures to meet those objectives and reduce those risks and any possible loss of confidentiality, integrity and availability

[36] For the first time, the General Data Protection Regulation (GDPR) addresses data protection by design as a legal obligation for data controllers and processors

that can compromise personal data. The choice of the countermeasures will depend on the outcome of the specific risk assessment[37].

71 For example: access controls ensure that only authorised individuals can read, modify or delete data in the system. Such controls help achieve confidentiality and integrity from a security perspective. Additionally, when an IT system processes personal data, the built-in controls should make sure that users can access only specific data to perform their duties. Access controls can thus help ensure that the use of personal data is limited to authorised purposes (purpose limitation) and data is protected from unauthorised access and tampering.

R9: Additional safeguards should be used such as encryption and multi-level access controls to mitigate high risk processing if an IT system processes especially sensitive (personal) data e.g. physical/mental health, racial/ethnic origin, political opinion, religious belief, criminal verdicts.

72 There may be various measures in place to achieve security. To access personal files, special passwords may be required. For identification of authorised users, distinct log-on procedures as well as logs recording file access and data changes should be introduced.

R10: Adequate measures should be designed into an IT system that allow adequate management of retention time and perform necessary subsequent actions such as e.g. anonymisation or deletion.

73 Opinion 5/2014 of the Article 29 Working Party on Anonymisation Techniques[38] "*concludes that anonymisation techniques can provide privacy guarantees and may be used to generate efficient anonymisation processes, but only if their application is engineered appropriately – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation while producing some useful data. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in this Opinion*".

5.3. Construction and Development (Do)

74 In the development phase, the code is written, and if the system contains hardware, then also its design and configuration will be considered to meet the requirements derived from the risk assessment.

[37] See for instance the EDPS guidelines on Security Measures for Personal Data Processing.

[38] Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques.

R11: A common understanding between the development team and stakeholders is important. The development team should be aware of data protection law and rules before the development phase starts. This can be guaranteed e.g. through training arranged with the DPO for the current and new development teams or equivalent measures.

75 The development team should document the system development in an easy to understand and comprehensive manner.

5.4. Test (Check)

76 The testing phase delivers feedback whether the system under development satisfies all requirements.

77 Data protection requirements should be considered in test cases and scenarios

78 Tests should also target all involved data protection requirements, including e.g. the existence of an exhaustive and clear data protection notice, the existence of features to manage data quality and cookies, privacy friendly default settings and IT security requirements.

79 An essential role can be played by an integrated security testing approach in the development phase (with security static code analysis and dynamic approaches such as penetration testing).

R12: Procedures and instructions on testing should be developed to ensure alignment with data protection requirements.

80 In the testing phase, sampling of real personal data should be avoided, as such data cannot be used for purposes for which it was not collected and using it in testing environments may result in making personal data available to unauthorised individuals.

81 Where possible, artificially created test data should be used, or test data which is derived from real data so that its structure is preserved but no actual personal data is contained in it. Different such techniques have been applied successfully[39].

82 Where thorough and cautious analysis shows that generated test data cannot provide sufficient assurance for the validity of the tests, a comprehensive decision must be taken and documented, which defines which real data shall be used in the test, as limited as possible, the additional technical and organisational safeguards which are established in the testing environment. Special categories of data can only be used in real data testing with the explicit consent of the individuals concerned.

[39] Test data generation techniques and tools are provided with several development environments.

R13: Sampling of real personal data during simulation of a "live" environment should be avoided.

83 Effective security safeguards should be taken into account when testing an IT system. If usage of real personal data is necessary for testing, it should be anonymised. The development of simulated datasets for general use by developers should be considered as an alternative.

84 Should there be a case in which personal data has to be used in the development or test environment, the requirements relevant for the production environment have to be applied.

85 In case a third party data processor under contract is involved in testing, special attention should be dedicated to data made available for testing purposes. Generally no real personal data should be used for this purpose.

86 Contractors should only have access to testing environments. If access to the production environment is necessary, only authorised IT administrators[40] of the respective institution should perform actions following instructions of the contractors, after the appropriate checks in the procedure have been performed. If only external IT administrators exist the controller should ensure that the contractor complies with the applicable data protection requirements.

5.5. Transition and Deployment (Act)

87 The main objective of this phase is to transfer the system from development to production. Users should understand the system. Therefore, activities of this phase should also include raising awareness on data protection for end-users and maintainers.

R14: The end users, system administrators and maintenance staff of the IT system should be aware of data protection rules.

5.6. Operations and Maintenance

88 Once an IT system has passed the acceptance testing phase and is cleared for production, it will become part of the standard operations of the organisation. The development team will hand over responsibility to the operations team. Development capacities will only be kept for maintenance purposes, i.e. the correction of errors discovered in productive operation and the implementation of limited adaptations of the system to changing requirements.

89 Unlike development of systems, which is usually organised in the form of projects and consists of many unique activities, systems operations is a day-to-day working process,

[40] A decision by a system owner should be required in order to be granted IT system administrator privileges.

which is performed continuously and repeats certain steps in regular intervals (e.g. backup, preparation, release upgrades, etc.).

90 Operations should work on the basis of comprehensive and current documentation of systems procedures, inter alia about specific requirements related to the processing of personal data.

91 If it is not yet done, an organisation should identify existing IT systems processing personal data, including different kinds of data (e.g. sensitive data such as health data). This should help to identify risks associated with the processing of personal data and to put in place an appropriate internal control system to ensure alignment with data protection law.

92 The assessment of the risks related to the operation of systems should be regularly reviewed and updated. An efficient practice is to integrate this as part of the regular risk management of the organisation operating the system.

R15: The controller should register with the Data Protection Officer of the institution any processing of personal data carried out via a database or an IT system.[41]

93 Privacy statements should be reviewed regularly in case of changes or additional services which involve the processing of personal data.

R16: The maximum retention time for data on storage media should be determined to ensure that it is in line with contractual, legal and regulatory requirements. The retention time may differ for different storage purposes.[42]

5.6.1. Information to data subjects and transparency

94 The institution has the obligation to provide the user of an IT system with information at least on the following elements of the processing operation:

a. The identity of the institution and of any other institution or entity sharing controllership responsibility and how to contact the institution for enquiries, requests and complaints.

b. Which personal data it is processing.

c. Why (purposes) the institution collects and further processes the data.

d. The recipients or categories of recipients of the personal data, by describing departments or categories of staff having access to the data.

e. Descriptions of transfers to other institutions or entities must also be indicated together with the reasons for the transfer.

[41] This notification has to be in accordance to Article 25 of Regulation (EC) No 45/2001.

[42] A backup will have different access controls and therefore risks than a regular operational system.

f. Clear indication of mandatory and optional information within the privacy statement, even though an online form exists designed to show mandatory and optional fields.

95 The information provided to the data subject should be:

a. Easily and directly accessible from the home page and any other page used to collect and process personal data

b. In clear and in plain language and

c. Clearly distinguishable from other legal and policy information.

96 The institutions should enable people with disabilities[43] to fully understand and effectively exercise their rights as data subjects if personal data is processed through IT services.

R17: The institution should develop appropriate information notices on the processing operations and use information channels to make this information accessible for the data subjects.

97 The appropriate information channel depends on the nature of the IT system and the interactions of data subjects with the institution. If the system is directly accessible to the individuals while data is processed (e.g. internal management systems for staff, or web services for external stakeholders) the system should provide the functionality for information about the processing via its user interface.

98 Where the data subjects cannot directly interact with the IT systems, the organisational processes must be designed so that the information is given at the right moment (e.g. when data is collected via a form, the form could provide information or a pointer to an information source).

99 The institution must also be able to provide the relevant information on demand, e.g. by providing a general request email address or web service, and a process to react to such demands within a reasonable time limit.

5.6.2. Access management[44]

100 It should be clarified who is the system owner and thus has the responsibility to ensure system risk management on a regular basis. The system owner also maintains appropriate access control as well as other risk mitigation controls and should ensure proper handling of IT security incidents and the disposal of the IT system.

[43] See e.g. for web services this page: http://www.w3.org/WAI/intro/accessibility.php.

[44] See also COBIT Version 5 A Business Framework for the Governance and Management of Enterprise IT for necessary control measures.

R18: User account management procedures should be established and implemented as well as approval procedures including granting access rights to a system by the system owner.

101 Management should regularly review access procedures and their effective implementation.

102 Access to personal data should generally be given according to the minimal privilege principle, i.e. only access rights necessary for performing a function should be allocated to users and administrators.

5.6.3. Change management

103 Controls should be put in place to limit the access to system components and to prevent unauthorised changes.

R19: Formal change management procedures should be established and implemented to handle in a consistent way all requests for changes to an information system.

104 Change management procedures should also be provided for contracted service providers (e.g. system development, application service providers).

105 In case of any change of purpose of processing personal data, data subjects should be informed about it and the legal basis of the changed purpose should be identified. The data protection requirements should be analysed with involvement of the DPO or equivalent function.

5.6.4. Security monitoring

R20: Access to files containing personal data should be monitored on a permanent basis.

Example: In case of bugs in system operation, the use of real personal data for code debugging should be avoided. In any case, if needed, an authorisation from the data controller needs to be obtained and both the authorisation process and the debugging actions need to be recorded and auditable. The amount of personal data used for testing should anyhow be minimised and a strict "need to know" policy applied.

106 Institutions should ensure that their IT systems are protected by using appropriate security technologies, that they implement the mitigation measures identified during the security risk assessment and that they are kept up-to-date to be able to meet any emerging threats.

107 The information systems should generate the necessary audit trails to allow the reconstruction of the sequence of events or changes in the IT system.

108 Note that if the security monitoring creates logging information it has to be assessed whether these logs contain personal data and thus need to be considered in the risk assessment. Therefore the purpose and the retention period need to be well defined.

109 Test and monitor the IT security implementation in a proactive way.

5.6.5. Data exchange

110 It is important to identify various scenarios where secondary use or data exchange with third parties may take place. Associated risks should be identified as it will be helpful in the definition and design of mitigation measures.

111 For detailed technical and practical guidance on transfers of personal data to third countries and international organisations by EU institutions see the relevant EDPS Position paper[45] and also Annex 2 on the processing by external organisations and transfers of personal data.

R21: Personal data should only be transferred via secure online channels. This can be achieved via trusted networks, using a channel where data is encrypted or equivalent means.

Example: When personal data are sent over public networks such as the Internet they need to be protected against threats inherent to those networks such as interception.

Encryption tools should be configured properly, together with a secure management of the relevant cryptographic keys.

112 Manual data transfers on removable unprotected physical media e.g. memory sticks, without strong encryption, should be avoided.

113 Transfer of Personal Data into a cloud based service or an online storage service without a proper security authorisation framework should be avoided. The use of such applications as e.g. “Dropbox” or “Google Drive” should be governed by appropriate risk management.[46]

Example: Email and word processing applications

Email and word processing tools are used in each institution. Their configuration should be so chosen that not more personal data than necessary is transferred, It may be necessary to ensure that hidden personal data is removed from files before transfers,

[45] EDPS Position paper of 14 July 2014 on the transfer of personal data to third countries and international organisations by EU institutions and bodies.

[46] Be aware that using of such service might imply transfer of Personal Data to a third country. See Annex 1 for more information.

114 Data controllers should put into place all necessary safeguards for using this software if personal data (such as HR, health data) is concerned.

> R22: Institutions using email to transfer sensitive personal data[47] should be aware of the inherent Data Protection issues of the technology which should be reflected in the Risk Assessment and ensure that this transmission is secured through e.g. encryption of a file, a secure email facility that encrypts the data including attachments or done only inside a trusted network.

115 Additional measures should be taken into account to prohibit or prevent the copying of personal data stored in applications to personal word processing applications.

5.6.6. Disposal[48]

> R23: Procedures should be established and implemented to ensure that requirements for the protection of personal data are met when software and hardware are disposed of or transferred to a different environment.

116 If an IT system becomes obsolete, is transferred or no longer in use, particular attention should be paid to preventing any possibility of unauthorised disclosure of personal data.

117 Agreed retention periods should be respected when disposing of an IT system.

118 Access to obsolete systems containing personal data should be removed where such an access is no longer necessary or cannot be justified.

119 Procedures and working instructions should be put in place related to disposal of electronic files containing personal data. Moreover, procedures should be put in place related to secure disposal of hardware (e.g. storage media).

5.7. Horizontal processes

5.7.1. Procurement and Outsourcing

120 When an IT system development is planned, it will be determined if any work will be outsourced or if standard software will be acquired for the system. Once the decision on outsourcing or acquisition is taken, a procurement process will be launched.

---

[47] Technically every email contains personal data. This recommendation is thus intended to cover additional personal data inside the actual message or subject.

[48] See also COBIT Version 5 A Business Framework for the Governance and Management of Enterprise IT for necessary control measures.

R24: The statement of work and other contract provisions should include technical and organisational safeguards that the contractor should fulfil to guarantee protection of the personal data being processed e.g. during the testing phase.

121 Specific model contractual clauses on data protection requirements could be used in this respect. Personal data processed in relation with procurement and related selection procedures should be protected according to the data protection rules[49].

122 The DPO/DPC should be involved in the procurement and support the process with their expertise.

123 If the decision is made to outsource the IT system, its development or other parts of the process the IT management should consider the additional risks and the limits to mitigation of these risks. As the controller the IT management will stay liable even when outsourcing and all the IT management should ensure that all the applicable recommendations given should be applied as far as possible by the party outsourced to.[50]

124 While the GDPR (Art. 25) provides a binding obligation to observe data protection by design and by default only for controllers, and does not apply directly to manufacturers and providers of standard products and services, in GDPR Recital 78 makes it clear that they should be encouraged to take the principles of data protection into account in development and design. The Recital also demands that "*The principles of data protection by design and by default should be taken into account in the context of public tenders*." EU Institutions should ensure that their procurement procedures for IT solutions are established accordingly.

5.7.2. Project management

125 Project management is the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements[51].

5.7.2.1. Roles and responsibilities

126 The responsible for data protection, e.g. DPO/DPC, should be involved in any new IT project that processes personal data through all its phases, as well as in identification of existing databases or applications that process personal data. They should be consulted to explain data protection requirements and to help verify if those requirements have been adequately designed and effectively implemented in the system in such a way that it complies with data protection law.

[49] EDPS Guidelines on the processing of personal data in the context of public procurement, grants as well as selection and use of experts.

[50] For detailed information on outsourcing consult the Annex 1.

[51] Definition according to PMI (Project Management Institute).

127 Their advice should also be requested in the inception phase of a project when it is to determine whether data processed via the IT system is personal data or not.

128 Also, their assistance is important for the identification and assessment of any risks related to the processing of personal data.

R25: The Project Manager of an IT project under development or the system owner should ensure proper communication with the responsible for data protection (DPO, DPC).

129 The project manager should also ensure that data protection requirements collected from the responsible for data protection are analysed properly and implemented into a system. Those requirements are gathered at the beginning of a project (inception and elaboration) phase.

5.7.2.2. Training on data protection requirements

130 The project manager, the project team (including the development team) and the staff in charge of operations and maintenance should attend training raising their awareness on applicable data protection rules organized with the DPO or be able to assure that they possess the required knowledge through other equivalent means. They should also be aware of privacy enhancing technologies and follow a privacy by design approach.

5.8. Standard Software

131 Standard software can be acquired on the market.

132 The entire life cycle of standard software should be considered: specification of requirements, selection of a suitable product, installation and customisation, testing, production release, and license management and disposal.

133 The following phases should be considered for bringing the standard software into service;

a. Planning - before choosing the standard software a list of requirements should be established. Based on this list the software can be selected in an objective and transparent manner. In this phase, in case of selection of more complex software, the responsible for procurement should also be involved. See section 5.1 and 5.2 and recommendations R6, R7, R8, R9 and R10.

b. Acquisition/Procurement - based on the established list of requirements it can be checked which existing product on the market has the most appropriate functionalities. See section 5.7.1, Annex 1 and recommendation R24.

c. Implementation/Test - it is necessary to test the functionalities specified in the documentation of the standard software. See section 5.4 and 5.5 and recommendations R12, R13 and R14.

d. Customization - in general the software will have to be customized according to the needs and legal obligations of the institution.

e. Installation - an effective license management and version control of standard software is necessary.

f. Operation and Maintenance - the processes and rules established during installation have to be kept in place and regularly reviewed. See section 5.6; 5.6.2; 5.6.3; 5.6.4; 5.6.5 and recommendations R15, R16, R17, R18, R19, R20, R21 and R22.

g. Disposal - an adequate disposal of the standard software requires very often complex and extensive work. See section 5.6.6 and recommendation R23.

6. THE THREE LINES OF DEFENCE MODEL

134 Good practice to improve oversight over an organisation is the internationally recognised model known to as the "Three Lines of Defence"[52]. This model may also be used as a reference in data protection to help set up an adequate governance framework and strengthen accountability in the organisation.

135 The three lines of the model are

1. Operational Management,
2. Risk Management Compliance Functions,
3. Internal Audit.

136 According to this model, senior management sets the "tone at the top" in the organisation and should emphasize the importance of the protection of personal data to all stakeholders that may interact with such data. Senior management should have specific responsibility for data protection and also designate a responsible for data protection.

137 To demonstrate compliance with data protection rules and to verify the effectiveness of the implemented measures, operational management defines appropriate processes as well as roles and responsibilities and establishes control activities upon the respective processes. All those elements belong to an internal control system in an organisation. Internal control systems should be designed to help an institution achieve its objectives[53].

138 Internal controls may consist inter alia of policies, procedures, technical and organisational safeguards, data protection impact assessments, codes of conduct and security and privacy certification.

139 Compliance functions of an organisation monitor whether controls comply with relevant data protection rules, while audit functions on the other hand provide independent assurance on the effectiveness and efficiency of the controls to senior management.

140 When establishing an internal audit work plan, it is recommended to ensure that the planning also covers processes and functions within the institution related to the processing of personal data and the responsibilities for the protection of personal data.

141 Such an audit exercise would provide an assessment of the adequacy and effectiveness of the internal control system for minimising the risk of violating data protection rules.

R26: Involve internal auditors in the assessment of the internal control system put in place to ensure alignment with data protection rules

[52] IIA Position Paper; the Three Lines of Defense in Effective Risk Management and Control, Altamonte Springs, FL: The Institute of Internal Auditors Inc, January 2013.

[53] Internal Control is broadly defined in the Financial Regulation (Article 32.2). This definition closely mirrors the standard definition of internal control adopted by COSO.

ANNEXES

Annex 1 Processing by external organisations and transfers of personal data

General considerations

142 EU institutions need to assess risks related to data protection if an IT service should be provided by a third party as well as the reliability of the third party concerning data protection and intelligence risks.

143 Personal data collected by EU institutions could be processed by organisations external to the institution because the institution uses the services of a contractor or of another external organisation to carry out its tasks. The external organisation therefore acts on behalf of the institution as a processor and Article 23 of the Regulation will apply.

144 However, if the external organisation processes the personal data collected by the EU institutions for its own purposes, the external organisation is also to be considered a controller, to whom data are transferred or made available. Rules of Articles 7, 8 and 9 of the Regulation will apply for those transfers of personal data[54].

145 Staff of the external organisation should be subject to the Memorandum of Understanding on security verification in order to have the insurance of reliability for assessing personal data.

146 The Regulation requires grounds for legitimacy of the processing at the external organisation and specific safeguards in both cases. The institution must identify the role of the prospective external organisation being involved in the personal data processing. Particular care should be taken in case of transfer of personal data to countries outside the EU/EEA and international organisations.

147 The rules of Article 9 of the Regulation will apply where data are made available to an external organisation outside the EU, irrespective of whether the recipient acts as processor or as additional controller. For detailed guidance on transfers of personal data to third countries and international organisations by EU institutions see also the relevant EDPS Position paper[55].

---

[54] A transfer of personal data should be considered to normally imply the following elements: communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it. These elements apply to transfers within or between EU institutions or bodies (Article 7), transfers to recipients subject to the Directive 95/46/EC / GDPR (Article 8) and to transfer to third countries and international organisations (Article 9). The term covers both deliberate transfers and permitted access to data by recipients. The conditions of knowledge and intention exclude cases of access through illegal actions (e.g. hacking). See section 3.1. of the EDPS Position paper on transfers to third countries.

[55] Position paper of 14 July 2014 on the transfer of personal data to third countries and international organisations by EU institutions and bodies.

External organisation acting as a processor

148 If the external organisation acts as a processor for the EU institution, then Article 23 of the Regulation on the relationships between controller and processor and the duties incumbent on the processor applies[56].

149 If the processor is an external organisation based outside the EU, Article 9 of the Regulation applies in addition to the provisions of Article 23. Where IT services are provided by a non-EU based organisation, it is important to take the provisions of Article 9 into consideration when choosing the processor and assessing the level of personal data protection provided by the processor.

150 The institution must ensure that the external processor will act only on its behalf and under its instructions in compliance with Article 23 of the Regulation. This has to be set up in a written contract between the institution and the processor with clear data protection provisions, including security, technical and organisational measures that the processor must put in in accordance with Articles 21 and 22 of the Regulation.

151 The institution is responsible for instructing the processor as to the security requirements and measures further to an IT risk assessment and to verify that the processor has set up those measures.

External organisation acting as a controller

152 In principle, EU institutions should avoid giving external entities the possibility to become a controller of personal data, unless this is necessary for their institutional objectives, e.g. when the EU institution cooperates with an international organisation in humanitarian or other areas.

153 Articles 7, 8 and 9 of the Regulation regulate transfers of personal data. Institutions can transfer personal data only when they are necessary and the recipients of the data transferred under Article 7, 8 or 9 of the Regulation must process the personal data only for the purposes for which they were transmitted.

154 If an external organisation acts as a controller, i.e. for their own purposes, it should assume all responsibilities related to controllership, including the obligations that personal data can be transferred only to recipients with an adequate level of protection and that data are transferred solely to allow the tasks of the controller to be carried out.

155 Institutions should provide the data subject with the following information to be transparent with regard to their IT services:

[56] Articles 7 and 8 of the Regulation do not apply if EU institutions make data available to a processor based in the EU, since this processor is working directly under the responsibility of the controller.

a. What processing operations are carried out by the organisation as a processor and which ones are carried out as a controller.

b. Any useful information about the data protection practices of the third party organisation in their capacity as controller.

Annex 2 Data protection recommendations in different phases of an IT system's life cycle

Life cycle phases of an IT system	Process and sub processes	Recommendations	General recommendation
Inception		**R6** As a starting point, it should be determined whether data processed via the respective IT system is personal data or not, or whether it can become personal data as the result of such processing.	**All life cycle phases of an IT system should comply with generally recognised data protection principles (see section 4.1)**
		R7 High level data protection requirements should be included in a project charter as this document contains the scope statement and high level requirements and is an outcome of the inception phase	
Elaboration	Requirements collection	**R8** Data protection requirements should be collected from stakeholders and documented in the IT system's specification phase	
	Design	**R9** Additional safeguards should be used such as e.g. encryption and multi-level access controls to mitigate high risk processing if an IT system processes especially categories sensitive of (personal) data e.g. physical/mental health, racial/ethnic origin, political opinion, religious belief, criminal verdicts.	
		R10 Adequate measures should be designed into an IT system that allow adequate management of retention time and perform necessary subsequent actions such as e.g. anonymisation or deletion	
Construction	Development	**R11** A common understanding between the development team and stakeholders is important. The development team should be aware of attend training raising its awareness on data protection law and rules before the development phase starts. This can be guaranteed e.g. through training arranged with the DPO for the current and new development teams or equivalent measures.	
	Test	**R12** Procedures and instructions on testing should be developed to ensure alignment with data protection requirements	
		R13 Sampling of real personal data during simulation of a "live" environment should be avoided	
Transition and Deployment		**R14** The end users, system administrators and maintenance staff of the IT system should be aware of data protection rules.	
Operations & Maintenance		**R15 The controller should register with the Data Protection Officer of the institution any processing of personal data carried out via a database or an IT system.**	
		R16 The maximum retention time for data on storage media should be determined to ensure that it is in line with contractual, legal and regulatory requirements. The retention time may differ for different storage purposes.	
	Information to data subjects	**R17** The institution should develop appropriate information notices on the processing operations and use	

Life cycle phases of an IT system	Process and sub processes	Recommendations	General recommendation
	and transparency	information channels to make this information accessible for the data subjects.	
	Access management	**R18** User account management procedures should be established and implemented as well as approval procedures including granting access rights to a system by the system owner	
	Change management	**R19** Formal change management procedures should be established and implemented to handle in a consistent way all requests for changes to an information system	
	Security monitoring	**R20** Access to files containing personal data should be monitored on a permanent basis	
	Data exchange	**R21** Personal data should only be transferred via secure online channels. This can be achieved via trusted networks, using a channel where data is encrypted or equivalent means.	
		R22 Institutions using email to transfer sensitive personal data should be aware of the inherent Data Protection issues of the technology which should be reflected in the Risk Assessment and ensure that this transmission is secured through e.g. encryption of a file or, a secure email facility that encrypts the data including attachments or done only inside a trusted network.	
	Disposal	**R23** Procedures should be established and implemented to ensure that requirements for the protection of personal data are met when software and hardware are disposed of or transferred to a different environment.	
Horizontal processes	Procurement	**R24** The statement of work and other contract provisions should include technical and organisational safeguards that the contractor should fulfil to guarantee protection of the personal data being processed e.g. during the testing phase.	
	Project Management	**R25** The Project Manager of an IT project under development or the system owner should ensure proper communication with the responsible for data protection (DPO, DPC).	
	Governance	**R1** It is of utmost importance that data protection principles should be unambiguously supported at management level.	
		R2 Senior management, if in the role of the controller, has to be accountable for data protection. If not in the role of the controller the Senior management should still take specific responsibility for Data Protection to ensure compliance with Data Protection rules.	
		R3 Senior management should take responsibility for data protection and also designate a responsible for data protection (e.g. Data Protection Officer, Data Protection Coordinator) and provide the responsible	

Life cycle phases of an IT system	Process and sub processes	Recommendations	General recommendation
		with a mandate to implement Data Protection policies.	
		R4 Existing policies and procedures on data protection should be well known by all staff. This can be ensured through e.g. mandatory induction training, provision of informative material or recurrent training.	
		R5 Policies, procedures as well as responsibilities and functions regarding data protection should be regularly monitored and maintained.	
		R26 Involve internal auditors in the assessment of the internal control system put in place to ensure alignment with data protection rules	