EUROPEAN DATA PROTECTION SUPERVISOR

# Guidance

## Security Measures for Personal Data Processing

## Article 22 of Regulation 45/2001

EDPS

21 March 2016

## Executive Summary

The EDPS aims in this guidance document at explaining Article 22 of Regulation 45/2001 and provides information on the main practical steps EU institutions and bodies should take in order to comply with it. It is based on generally accepted good practices in **Information Security Risk Management (ISRM)** and aims at helping EU institutions, as controllers, to assume their responsibility according to the accountability principle.

Securing information is a key objective that any organisation must manage in order to fulfil its stated mission. Moreover, most organisations must deal with an ever changing landscape affecting their operations. Uncertainties created by such changes will affect how the organisation needs to react in order to ensure that its information assets are suitably protected. Therefore, there is a need for a specific framework that helps individuals responsible for information security to manage the uncertainties which might affect the security of their organisation's information over time. Such framework for a specific organisation is referred to as **ISRM process**.

In the **context of processing personal data**, risks must be mitigated as per the legal requirement stated in Article 22 of Regulation 45/2001 which means that

- In its analysis, Information Security Risk Management must also cover information security risks affecting personal data
- From it analysis, a set of suitable security measures may be defined and implemented

Security measures protecting personal data cannot be defined generically since they must come from the Information Security Risk Management process, which takes into account the specific context in which personal data is processed.

Implementing a proper ISRM process implies at least the following:

1. Having management buy-in and approval on the ISRM process itself as well as providing guidance on the acceptable levels of risks.
2. Allocating resources to tackle all tasks related to ISRM.
3. Providing adequate training and awareness to staff on the existence and implementation of the ISRM process.
4. Linking the ISRM process to other processes of the EU institution as appropriate.
5. Following risk assessments, analysing possible security measures and selecting the most appropriate ones based on security, data protection and needs.
6. Regularly reviewing all steps of the ISRM process, in the light of the changes to the operations and to the risks to information including **personal data** processed by the EU institution. This includes reviewing the implementation of security controls and their suitability in the light of technology and market developments, as well as taking into account the changes in the processing of personal data by the EU institution.
7. Efficiently documenting all key steps of the ISRM process and making use of tools to ease the implementation of all steps of that process.
8. As quickly as possible, reviewing current security measures for existing processes and IT systems in order to align them with the appropriate risk assessments.

## TABLE OF CONTENTS

# 1 Introduction

## 1.1 Aim and scope of this document

This document aims at explaining Article 22 of Regulation 45/2001[1] ("the Regulation") and providing guidance for EU institutions and bodies ("EU institutions) on the main concept described in this article.

The document is targeted at the EU institutions' management and staff responsible for securing the processing of personal data through technical and organisational measures, as well as the staff members monitoring and ensuring compliance with data protection obligations.

It is based on generally accepted good practices in **Information Security Risk Management** and aims at helping EU institutions, as controllers, to assume their responsibility according to the accountability principle[2].

The provisions under Article 22 of the Regulation are analogous in substance to the ones contained in other data protection legal instruments (e.g. Directive 95/46/EC; Directive 2002/58/EC; Council Framework Decision 2008/977/JHA). Thus the approach layed out in this document should also be useful for bodies, organisations or companies that are subject to these other legal instruments.

In the legal text of Article 22 [see box below] **emphasis** is added to indicate the references to Information Security Risk Management:

> *Security of processing*
>
> 1. *Having regard to the state of the art and the cost of their implementation, **the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.***
>
>    *Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.*
>
> 2. *Where personal data are processed by automated means, measures shall be taken **as appropriate in view of the risks** in particular with the aim of:*
>
>    a. *preventing any unauthorised person from gaining access to computer systems processing personal data;*
>
>    b. *preventing any unauthorised reading, copying, alteration or removal of storage media;*
>
>    c. *preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;*
>
>    d. *preventing unauthorised persons from using data-processing systems by means of data transmission facilities;*
>
>    e. *ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;*
>
>    f. *recording which personal data have been communicated, at what times and to whom;*
>
>    g. *ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;*
>
>    h. *ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;*
>
>    i. *ensuring that, during communication of personal data and during transport of storage media, the data*

[1] 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

[2] Article 29 WP 173, Opinion 3/2010 of 13/07/2010

*cannot be read, copied or erased without authorisation;*

j. *designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.*

Information Security Risk Management is a concept broader than the processing of personal data. A description of that concept is provided for the reader in chapter 1.2 – the reader should note however that in the **context of processing personal data**, risks must be mitigated as per the legal requirement stated in Article 22 of Regulation 45/2001 which means that

- In its analysis, Information Security Risk Management must also cover information security risks affecting personal data;
- From it analysis, a set of suitable security measures may be defined and implemented (see also chapter 1.2.2.2).

Security measures protecting personal data cannot be defined generically (it is not possible to define a set of security measures that can be applied in all cases) since they must come from the Information Security Risk Management process, which takes into account the specific context in which personal data is processed.

## 1.2 Background

### 1.2.1 The ‘bigger picture’

Securing information is a key objective that any organisation must manage in order to fulfil its stated mission. This key objective is associated with a specific field of knowledge called "Information Security" which refers to the processes and methodologies which are designed and implemented to protect printed, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.[3]

It should be noted that Information Security applies irrespective of the nature of the information; its key concepts apply whether or not personal data is processed. They are recalled here to provide background and complement the reading of Article 22 of the Regulation.

Most organisations must deal with an ever changing landscape affecting their operations. Uncertainties created by such changes will affect how the organisation needs to react in order to ensure that its information assets[4] are suitably protected.

Furthermore, individuals responsible for their organisation's Information Security would need to fulfil their task and manage these uncertainties with a limited set of resources and often tight deadlines stemming from the organisation's needs.

Therefore, there is a need for a specific framework that helps individuals responsible for information security to manage the uncertainties which might affect the security of their organisation's information over time and indicates how to best react to these uncertainties within the constraints of their work environment (e.g. with the staff working in the organisation, within their budget, within their time constraints, management strategy etc.). This framework would also serve to help sharing views on the necessary activities that need to be carried out in order to ensure proper Information Security within the organisation. Such

[3] https://www.sans.org/information-security/

[4] An information asset is a piece of data which has value to the organisation (e.g. an employee record, analysis reports, financial data of the organisation, etc.)

framework for a specific organisation is referred to as **Information Security Risk Management process**.

Security measures can only be defined and implemented **in the final phase of** the Information Security Risk Management process, otherwise, an organisation has no guarantee that the selected security measures are adequate or sufficient in order to mitigate the risks to a level acceptable by the organisation’s management.

### 1.2.2 Basis of Information Security Risk Management (ISRM)

#### 1.2.2.1 Overview

A possible framework[5] to manage uncertainties which might affect the security of an organisation's information has been defined by ISO[6] as **Information Security Risk Management (ISRM)**. ISO views the ISRM as a continual process that aims to "… assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions"[7].

In order to fully understand what is meant by ISO by this definition of ISRM, it is necessary[8] to also make reference to the definition[9] of "risk" as "effect of uncertainty on objectives". In this context, we are focused on the objective to secure **information**. Accordingly, in the context of this document, we are only interested in risks to Information Security.

Figure 1 gives an overview of the **ISRM process**. Each step is summarily described in the next subchapters.

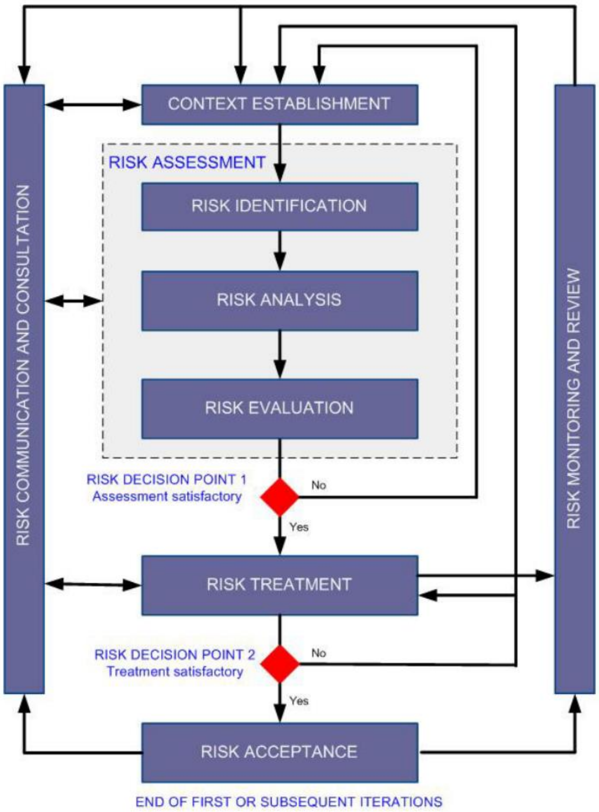

**Figure 1: overview of Information Security Risk Management**

[5] Other frameworks exist such as NIST SP 800-39 or COBIT (ISACA)

[6] See ISO 27005

[7] ibidem

[8] Although ISO 27000 and ISO 27005 provide a bigger set of definitions, the ones formalised here are the ones essential for understanding the rest of this document.

[9] See chapter 5

Basically, ISRM is achieved by iterating through each step [as shown on Figure 1], i.e. going through each step and then starting again once the full process has finished. Each iteration uses the previous results as a stepping stone. The first iteration is of course the most expensive in terms of resources as there are no previous results to build upon. However, it should be noted that going through subsequent iterations requires investment and commitment from the organisation.

This exercise allows the organisation to:

- Identify the risks to the organisation and assess the consequences of these risks to the operations.
- Make informed decisions on how to react with regards to these risks.
- Prioritise actions in order to deal with these risks.
- Effectively monitor its activities.
- Raise staff awareness on Information Security.

#### 1.2.2.2 The steps of Information Security Risk Management

This chapter summarises each step shown in Figure 1. The reader is encouraged to consult ISO 27005 for more detailed information.

##### ***A Context Establishment***

This step serves to launch an iteration of the ISRM process. All relevant information is collected, the elements to carry out the rest of the exercise are defined (e.g. risk evaluation criteria, impact criteria, etc.), the scope and objective of the ISRM is defined and responsibilities are assigned to key staff in order to carry out the exercise.

##### ***B Risk Assessment***

Taking the information collected and defined in the previous "Context Establishment" step, "Risk Assessment" aims at identifying and describing the risks the organisation is subject to by performing the following steps:

###### B.1 Risk Identification

The goal of this step is to determine what risks can affect the organisation (i.e. to determine what can go wrong, how it can go wrong, and understand why this could happen). For this identification to be meaningful, the previous analysis of the specific context [1.2.2.2 A] of the organisation is of paramount importance.

###### B.2 Risk Analysis

Once a set of risks has been identified, each risk is analysed in order to determine the probability that this risk materialises and the consequences it may then have on the organisation.
There are several risk analysis methodologies available such as EBIOS[10], Octave/Octave Allegro[11], MAGERIT[12]. The selection of an appropriate methodology is done in the "Context Establishment" step [1.2.2.2 A]

[10] http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[11] http://www.cert.org/resilience/products-services/octave/

[12] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

### B.3 Risk Evaluation

Each risk that has been analysed and estimated in the previous step is then compared against criteria defined in the "Context Establishment" step. The evaluated risks are then prioritised in order to feed the next step.

### *C Risk Treatment*

Once risks have been evaluated and prioritised, a decision on what to do with each risk needs to be taken by the organisation. Typically, an organisation may decide **to reduce** the risk (by implementing, changing or removing security measures); **to retain** the risk (i.e. keep the situation as it is); **to avoid** the risk (decide to avoid an activity in order to avoid that risk); **to share** the risk (use an external party that could better cope with managing that risk). These decisions are not mutually exclusive.

After decisions have been taken, a risk treatment plan is devised (**i.e. security measures are defined with a plan on how and when they need to be implemented**). Additionally, the residual risks are estimated (i.e. after treatment, a risk is usually not completely eliminated; it is thus necessary to evaluate the level of this remaining risk).

### *D Risk Acceptance*

If the residual risks are deemed acceptable by the organisation, a formal decision by the organisation's decision makers is recorded. Otherwise, further analysis or treatment is performed.

Following this process, ultimately, the organisation's decision makers **take the responsibility** to deal with risks taking into account the organisation's overall strategy and available resources. Security measures may therefore be implemented or not depending on whether the acceptable level of risks for the organisation is reached.

### *E Risk Communication and Consultation*

This step aims at communicating risk related information (the risk analysis, evaluation, treatment and acceptance) to all stakeholders in order to achieve a ‘buy-in’ (acceptance) on the practical activities to take in order to deal with the risks. This means that stakeholders are aware and committed to do ‘whatever it takes’ to implement the measures foreseen under the security plan. This step also ensures that the appropriate information is considered throughout the ISRM.

### *F Risk Monitoring and Review*

As with any security-related activity, risks need to be constantly monitored in order to react appropriately to changes to the risks and adapt the appropriate parts of the ISRM accordingly.

Furthermore, the ISRM process itself should be reviewed and improved so that any subsequent iteration is more effective and efficient.

# 2 Interpretation of Article 22 of the Regulation

As pointed out by the emphasized sections above in Article 22, and, in particular, under Article 22(1), the need for measures has to be analysed in light of the need to ensure a level of security appropriate to the "**risks represented by the processing"** of personal data performed by the EU institutions and bodies and the nature of the personal data processed.

Explicitly mentioned are risks to confidentiality (*unauthorised disclosure or access)*, integrity (*unlawful ... or accidental ... alteration*) and availability (*accidental or unlawful destruction or accidental loss*), but other risks also have to be considered (*all other unlawful forms of processing).* All the identified risks must be mitigated and thus appropriate security measures must be implemented.

The ISRM must cover all manual or automated processing operations, and all factors of relevant risks posed by the processing, taking into account not only the systems more directly used for the processing but also infrastructural and environmental elements, such as physical security, energy supply/network, buildings access and other factors[13].

Both paragraphs 22(1) and 22(2) underline the importance of risk management. They also indicate (see wording "in particular") that **the risks** listed in paragraph 1 and **the security objectives** listed in subparagraphs 2(a) to (j) are to be considered in the context of the risk assessment and that these lists are **neither exhaustive** nor **prescriptive**.

The list is not exhaustive because there may be **additional risks** not explicitly mentioned under Article 22, but still relevant for certain specific processing operation; and, it is not prescriptive since there may be security objectives which are **only relevant for specific** operations.

Since paragraph 22(2) is not exhaustive, it cannot be relied upon as a check-list ensuring security of processing. Nonetheless, we see that the security objectives under Article 22(2) apply to all **automated** processing operations, and therefore as a rule the respective security controls need to be implemented (unless, in a given context, justification is provided and properly documented and approved by the management on why a specific item in the 'Article 22(2) list' does not raise the need for such security controls).

In order to properly comply with the legal obligation under Article 22 of the Regulation and meet all the security objectives under letters (a)-(j) of Article 22(2), EU institutions must always apply state of the art **risk assessment** and **risk management**.

**Appropriate security measures can only be derived from this process of risk management.**

Ultimately, management is accountable for the decisions to be taken according to the state of the art and concerning in particular[14]:

- risk treatment (in broad terms, these decisions relate to whether accepting, reducing, transferring or avoiding risks),
- the security measures selected and implemented to reduce the risks, and
- the residual risks (i.e. the risks which remain after the implementation of the selected security measures).

[13] On the **timing** of the 'implementation of the security measures, we note that Directive 95/46/EC under Article 17 contains provisions which are similar to the ones contained under Article 22 of the Regulation. In particular, recital 46 of the Directive clarifies that the security measures have to be taken "both **at the time of the design of the processing system** and **at the time of the processing** itself".

[14] As documented in the following standards: ISO 27005, BSI standard 100-3, NIST special publication 800-30…

The Regulation (as other data protection legal instruments) refers to costs as a factor: this requires careful evaluation. A **comprehensive cost-benefit analysis** should be used to assess the security measures to be chosen, where appropriate also considering different options to be implemented. In practice, most security measures will serve **more than one security objective** and thus will create benefits for the EU institutions which go beyond compliance with data protection obligations (ensuring security in a broad sense, that is, also when personal data are not 'at stake'). In other words the cost-benefit analysis should take into account such 'synergies of benefits' (costs must not be considered 'in isolation').

Since threats, technologies, processes and other factors relevant for the **risk assessment** evolve constantly, it is necessary for EU institutions to regularly review their **risk assessment** and the selection of **security measures**. Thus, the EU institutions should implement a robust **ISRM** process covering the security risks on their processing of personal data over time.

The ISRM process would provide the full set of justifications for and details on what security controls are implemented for a given data processing operation in the specific circumstances of the case.

# 3 Implications for the EU Institution

Implementing a proper ISRM process implies at least the following:

(1) Having management buy-in and approval on the ISRM process itself as well as providing guidance on the acceptable levels of risks. This also includes selecting an appropriate risk assessment[15] methodology and applying it consistently. In order to ensure that the state of the art is taken into account, consideration should be given to recognised standards[16] for performing risk assessments.

(2) Allocating resources to tackle all tasks related to ISRM.

(3) Providing adequate training and awareness to staff on the existence and implementation of the ISRM process (including on the risk assessments and on the selected security controls).

(4) Linking the ISRM process to other processes of the EU institution as appropriate. For example: (i) some processes such as security incident management (the procedure for the handling of security and data breaches) should feed the ISRM process; (ii) the ISRM process needs to adapt to the changing strategy laid out by management and to the overall organisation's risk management process[17].

(5) **Following risk assessments**, analysing possible security measures and selecting the most appropriate ones based on security, data protection and needs. Furthermore, the implementation of the selected security controls, as the rest of the ISRM process, needs to be planned appropriately, involving all stakeholders as necessary. Stakeholders would typically include staff members having the following functions: the Information Security Officer, the Security Officer, the Data Protection Officer, the Documents Management Officer and other process owners, the project officers and any other decision makers

[15] ISO 27001 definition: systematic use of information to identify sources and to estimate the risk, and to compare the estimated risk against given risk criteria to determine the significance of the risk

[16] Such as ISO 27005, BSI standard 100-3, EBIOS, Octave Allegro, NIST special publication 800-30, MAGERIT…

[17] This document focusses on Information Security Risk Management. An organisation would typically also deal with **overall Risk Management** (often referred to as **Enterprise Risk Management**), which is the process designed to identify potential events that may affect the entity, and manage risks: such process goes beyond looking at the information the organisation processes and the security of this information. In this regard, see ISO 31000.

(management). The Information Security Officer and the Data Protection Officer, specifically, should always be involved in the ISRM process.

(6) Regularly reviewing all steps of the ISRM process, in the light of the changes to the operations and to the risks to information including **personal data** processed by the EU institution. This includes reviewing the implementation of security controls and their suitability in the light of technology and market developments, as well as taking into account the changes in the processing of personal data by the EU institution (for example, the starting of the processing of sensitive data).

(7) Efficiently documenting all key steps of the ISRM process and making use of tools to ease the implementation of all steps of that process.

(8) As quickly as possible, reviewing current security measures for existing processes and IT systems in order to align them with the appropriate risk assessments.

# 4 Distribution of the main ISRM tasks

ISRM is a complex process covering all information processed by an organisation (including personal data) and requiring very specific expertise. Thus, several profiles would need to work together in order to ensure an optimal result.

The tables below provide some guidance on which function should perform the main ISRM tasks. Depending on the exact definition of functions within an organisation, these allocation of tasks may vary.

| **Management** |
|---|
| - Allocate resources for the ISRM<br>- Provide input to build the ISRM framework<br>- Approve all documentation related to the ISRM<br>- Decide on the risk treatment<br>- Agree to the residual risks<br>- Support the implementation of security controls by allocating budget and resources<br>- Take into consideration input from the Data Protection Officer with regards to the need for protection of personal data |

| **Information Security Officer (typically LISO in the EU Institutions)/Security Officer** |
|---|
| - Main responsible function for the ISRM<br>- Document the ISRM<br>- Iterate the ISRM process over time<br>- Perform the Risk assessments<br>- Draft all documents related to the ISRM<br>- Present results to management<br>- Implement management's guidance/decisions on the ISRM<br>- In light of the ISRM and management's decisions, determine the most suitable security control<br>- Follow up on the implementation of security controls<br>- Provide training and raise awareness on all aspects related to the ISRM |

**The Data Protection Officer**

- Support the ISRM with his specific expertise on risks associated to personal data processing
- Review ISRM documentation
- Provide input as to the most suitable security controls when personal data is concerned
- Discuss with Management the need to reduce risks related to the processing of personal data

**Process owners and IT operations**

- Support the ISRM process
- Provide input for the ISRM and the risk assessments
- Review ISRM documentation
- Provide input as to the most suitable security controls in a given context
- Implement the security controls

Done in Brussels, 21 March 2016

**(Signed)**

Wojciech Rafał WIEWIÓROWSKI

Assistant European Data Protection Supervisor

# 5 Glossary[18]

| | |
|---|---|
| **Availability** | Property of being accessible and usable upon demand by an authorized entity |
| **Confidentiality** | Property that information is not made available or disclosed to unauthorized individuals, entities, or processes |
| **Control** | Measure that is modifying risk |
| **Control objective** | Statement describing what is to be achieved as a result of implementing controls |
| **Information security** | Preservation of confidentiality, integrity and availability of information |
| **Integrity** | Property of accuracy and completeness |
| **Level of risk** | Magnitude of a risk expressed in terms of the combination of consequences and their likelihood |
| **Residual risk** | Risk remaining after risk treatment |
| **Risk** | Effect of uncertainty on objectives |
| **Risk acceptance** | Informed decision to take a particular risk |
| **Risk analysis** | Process to comprehend the nature of risk and to determine the level of risk |
| **Risk assessment** | Overall process of risk identification, risk analysis and risk evaluation |
| **Risk communication and consultation** | Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk |
| **Risk criteria** | Terms of reference against which the significance of risk is evaluated |
| **Risk evaluation** | Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable |
| **Risk identification** | Process of finding, recognizing and describing risks |
| **Risk management** | Coordinated activities to direct and control an organization with regard to risk |
| **Risk management process** | Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk |
| **Risk treatment** | Process to modify risk |
| **Threat** | Potential cause of an unwanted incident, which may result in harm to a system or organization |
| **Vulnerability** | Weakness of an asset or control that can be exploited by one or more threats |

[18] See ISO 20000:2014