

**Risk Management and Impact Assessment**

**in the Processing of Personal Data**

**LIST of TABLES**

June 2021



This work is licensed under a Creative Commons Atribución-NoComercial-CompartirIgual 4.0 License

International.

TABLE OF CONTENTS OF TABLES

Table 1 Examples of different perspectives on risk management 15

Table 2 Examples of Legal Safeguards and their relation to Risk Management 20

Table 3 Properties to be met by Well-Defined Processing Purposes. 30

Table 4 Example of Information describing the Processing that is Useful for Risk Management. 32

Table 5 Classification of Risk Management Measures and Safeguards 39

Table 6 Measures and Safeguards for Risk Management based on the GDPR 40

Table 7 Example: Personal Data Breach Scenario 45

Table 8 Factors that determine the Degree of Resilience of an Organisation 48

Table 9 Characteristics of Risk Management Documentation 58

Table 10 Minimum content of Risk Management Documentation 59

Table 11 Information derived from a High-Level Processing Analysis 66

Table 12 Description of a Processing Phase 69

Table 13 Description of assets involved in processing 72

Table 14 Likelihood x Impact Matrix to determine the Level of Risk 76

Table 15 Criteria for determining the Level of Impact 77

Table 16 Criteria for determining the Likelihood of Materialisation of a Risk Factor 78

Table 17 Categories of Risk Factors identified in the GDPR or in its development. 80

Table 18 Risk Factors associated with the Operations related to the Purposes of Processing. 83

Table 19 Risk Factors associated with the Types of Data used in the Processing. 88

Table 20 Risk Factors associated with the Extent and Scope of Processing. 89

Table 21 Risk Factors associated with Data Subject Category. 90

Table 22 Risk Factors associated with Technical Processing Factors. 91

Table 23 Risk Factors associated with Data Collection and Generation. 92

Table 24 Risk Factors associated with Processing Side Effects. 93

Table 25 Risk Factors associated with Category of Controller/Processor. 94

Table 26 Risk Factors associated with Data Disclosure. 95

Table 27 Description of a Personal Data Breach Scenario. 96

Table 28 Compilation of Impact Level for cases of Personal Data Breaches. 96

Table 29 Compilation of Likelihood of Personal Data Breaches Materialising. 97

Table 30 Evolution of the Likelihood of a data breach materialising over time 97

Table 31 Likelihood x Impact Matrix to determine the Level of Risk of a Personal Data Breach 98

Table 32 Possible Relationship between Impact and Likelihood on data breaches subject to the Volume of Data. 98

Table 33 Analysis of the Assets involved in the Processing. 99

Table 34 Examples of other Possible Risk Factors 101

Table 35 Examples of High-Impact Cases 102

Table 36 Examples of Possible Measures on the Processing Concept 106

Table 37 Examples of possible Data Protection Policies and Governance Measures 112

Table 38 Objectives of Privacy Protection “by Design”. 112

Table 39 Data Protection Strategies, Description, Tactics, Controls and Patterns by Design. 117

Table 40 Correspondence between the Level of Risk to Rights and Freedoms and category of the National Security Framework 118

Table 41 Selection of Security Measures. 123

Table 42 Specific Controls in the processing of Personal Data Breaches. 124

Table 43 Resilience-Related Controls. 124

Table 44 Controls relating to Failures in the Technical Safeguards for Data Protection and Errors in Applications 125

Table 45 Assessment of Residual Risk vs. Intrinsic Risk. 128

Table 46 Elements triggering a risk management review cycle. 129

Table 47 Obligation to carry out the DPIA 135

Table 48 Judgement of Suitability, Necessity and Proportionality in the Strict Sense. 140

Table 49 Minimum information required in the assessment of the necessity and proportionality of processing. 147

Table 50 Minimum requirements for the submission of a prior consultation. 154

|  |  |
| --- | --- |
| **Examples of different perspectives on risk management** | |
| The processing itself | Financial risk |
|  | Project risk |
|  | Fraud risk |
|  | Safety risks to persons (occupational) |
|  | Cost/benefit |
|  | Technical reliability risk |
|  | Business continuity risks in I.S., etc. |
| Processing in the internal context of the organisation | Impact on other processing in the same organisation, directly or indirectly |
|  | Opportunity cost, etc. |
| Processing in the external regulatory, social and economic context | Legal and compliance risk |
|  | Risks of civil or criminal liability |
|  | Environmental risk |
|  | Social impact |
|  | Risk to rights and freedoms, etc. |

Table 1 Examples of different perspectives on risk management

|  |  |
| --- | --- |
| Legal Guarantee | Management of the risks posed to rights and freedoms. |
| Contract with the processor  complying with the requirements of Article 28 of the GDPR | It is a regulatory compliance obligation, not risk management |
| Insurance policy to cover the  organisational responsibility for a possible breach of the GDPR | It involves risk management of  compliance, but not with regard to rights and freedoms. |
| The signing of a confidentiality agreement by personnel processing certain data. | It can be a risk management measure for rights and freedoms, insofar as it does not relax the obligations of the responsible party, but seeks to ensure the  commitment of the personnel processing the data. |

Table 2 Examples of Legal Safeguards and their relation to Risk Management

|  |  |
| --- | --- |
| Ultimate | The ultimate goal of the processing must be determined and not confused with intermediate goals, instrumental means or processing operations that take place at some stage of the processing or that may be dependent on the form of implementing the processing 1. |
| Specific | Sufficiently precise and concrete, specifying gaps, demands, requirements, obligations or opportunities  objective and final objectives that the end of the processing comes to resolve or to respond to. |
| Measurable | They must define a desirable future state in qualitative terms. |
| Achievable and realistic | Guarantees are determined in order to achieve the purposes of the processing to the extent that it is possible to "demonstrate" that the ultimate goal will be achieved. |
| Limited | The purposes are to be achieved over a period of time and within a given stage of the processing lifecycle. |

Table 3 Properties to be met by Well-Defined Processing Purposes.

1 In case it is used in a processing, e.g. video surveillance, it does not imply that the purpose of the processing is video surveillance. The purpose could be to preserve the security of persons, to control access to an enclosure or any other purpose. Video surveillance operations are a means and a concrete implementation of such processing aimed at achieving this end.

|  |  |  |  |
| --- | --- | --- | --- |
| **PURPOSE OF THE PROCESSING OPERATION** | | | |
| **Its purpose** | **Its nature** | **Its scope** | **Its context** |
| * Ultimate purposes. * Instrumental purposes. * Secondary purposes. * Other. | * The stages at which it is implemented. * The flow of personal data. * The processing operations required (manual and automated). * The assets/elements on which it is implemented. * The roles accessing the data. * The relevant technological features. * The involvement of processors in various operations. * Other. | * The extent of the amount of data. * The extent of the number of subjects affected. * The extent of data types and categories. * The geographical extent. * The extent of time of processing. * The extent in time of conservation. * The frequency of collection. * Granularity. * Other. | * The market or sector in which it operates. * The social environment in which it is deployed. * The regulatory environment. * The interaction with other processing of the entity. * The transfers of data that are necessary. * The international transfers involved. * The data breaches or incidents that occur in related processing. * The collateral effects on society * Other.. |

Table 4 Example of Information describing the Processing that is Useful for Risk Management.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Management of the Risks posed to Rights and Freedoms.** | | | | |
| Proactive/ preventive | Legal safeguards | Technical safeguards | Organisational safeguards | Reduce/ mitigate |
| Detection | Avoid/eliminate |
| Reactive/ corrective | Accept/ assume |

Table 5 Classification of Risk Management Measures and Safeguards

|  |  |
| --- | --- |
| Measures and safeguards based on the GDPR | Measures on processing concept and design. |
| Governance and policy measures |
| Data protection measures by default2 and by design |
| Personal data breach prevention and management measures / security measures. |

Table 6 Measures and Safeguards for Risk Management based on the GDPR

2 It should be remembered that default data protection measures have to be implemented by default, i.e. in any case and irrespective of the risk. See [Guide to Data Protection by Default.](https://www.aepd.es/media/guias/guia-proteccion-datos-por-defecto.pdf)

|  |  |
| --- | --- |
| **Processing based on**  **home automation or consumption control applications** | **Scenario 1** |
| Breach materialised: | Confidentiality: access to the records of  activity of the users of the home automation systems that are stored on a central server. |
| Compromised data: | Basic data, contact data, detailed data on system events, usage or consumption per minute over a long period of time. |
| Damage to the data subject: | The user's address and identification details are known.  It could be inferred when the household is empty.  The times of entry and exit from the household could be inferred.  It could be inferred whether the individual lives alone or in company.  It could be inferred when they go to sleep.  Very personal aspects, and even special categories of data, can be inferred.  Etc. |
| Assessment of the impact on the data subject: | It can have a very significant impact, affecting fundamental rights and freedoms in an irreversible way. |
| Measures to reduce the impact: | Reduce the temporal precision of data collection, and instead of collecting data by the minute, collect data by hours, days, or weeks (reduce granularity) Group data from different individuals (increase aggregation).  Reduce the dataset collected (data minimisation).  Delete individually collected information in a very short space of time, almost real time (data storage).  Have a very rapid procedure for communicating to those affected (data breach disclosure).  Etc. |
| Measures to reduce the likelihood: | Identification measure for access to the system. Data access control systems.  Encrypt information in transit and at rest.  Etc. |

Table 7 Example: Personal Data Breach Scenario

|  |  |
| --- | --- |
| People capability | Staff, from the highest to the lowest level, must have the ability to detect change, the ability to communicate change, the ability to understand change, the ability to innovate in the face of change, the ability to act and the willingness to act proactively, in  real time. |
| Adequate flow of information | It must be agile, specific, minimal, complete and from and to the adequate people  . |
| Leadership | There must be clear decision-making points with responsibilities and accountabilities  that are well defined. |
| Strategic adaptability | Physical, technological and organisational structures need to be able to evolve in real time towards new objectives or  ways of acting. |

Table 8 Factors that determine the Degree of Resilience of an Organisation

|  |  |
| --- | --- |
| It is a working tool | It should be useful for the effective implementation of risk management. |
| It must be efficient | It should place a minimal burden on processing management. |
| It must be complete | It shall record the risk management decisions taken, as well as the justification for these decisions based on objective evidence  . |
| It must be dynamic | It must be maintained and evolve as changes occur in the processing, in its context or incidences affecting it. |
| It must be traceable | It will allow the risk management process to be monitored and how it evolve over time. |
| It must be reportable | It must reach the appropriate decision-making  , decision implementation and control bodies. |
| It has to transmit information | It must have the format, language and content necessary for such actions to be implemented effectively and efficiently |
| It is not monolithic | It should be made up of different documents, adapted to the different recipients of the information. |
| It must be integrated into the management of the organisation | In line with what has been stated in relation to data protection policies, it must be integrated with the rest of the documentation associated with the management of data processing in other  aspects. |

Table 9 Characteristics of Risk Management Documentation

|  |
| --- |
| 1. Who performs it. |
| 1. Who approves it. |
| 1. The description of the processing. |
| 1. Methodologies and guidelines used in the management process. |
| 1. Identifying and analysing risk rights and freedoms. |
| 1. Assessment of level of risk posed to rights and freedoms. |
| 1. The decision whether or not to conduct a DPIA (analysis of obligation and analysis of need for DPIA). |
| 1. The selected measures and an implementation and monitoring plan. |
| 1. Criteria for re-evaluating the plan and timelines for revising the plan |
| 1. Incidents detected |
| 1. Date of completion or revision. |

Table 10 Minimum content of Risk Management Documentation

|  |  |  |
| --- | --- | --- |
| **Processing** | | Name or description |
| Controller/s | | Identification of the controller3. |
| **Processing purposes** | | |
| Purpose of the processing | |  |
| Intermediate and secondary purposes4 | |  |
| **Scope and field of processing** | | |
| Personal data | | |
| Personal data processed | | Grouped by category. |
| Data accuracy | | Including, at least:   * The frequency of collection. * Granularity. |
| Life cycle of data | | A brief description of its life cycle, including:   * Conditions for erasure of data. * Maximum and minimum time the data may be kept for processing. |
| Data subjects | | |
| Categories of data subjects affected | | Establish the possible categories of data subjects for whom the processing is intended to be designed (minors, people at risk of social exclusion, patients, pupils, etc.). It is recommended to analyse possible power imbalances between the data subjects and the  Data controller5. |
| Volume of subjects | | Number of subjects affected. |
| Geographical extent | | Local, regional, national or international. Specifying this extent. |
| Duration of the processing | | |
| Extension of processing time | | Both from the start of production to the proposed withdrawal of processing.  Description of circumstances that could lead to withdrawal of processing. |
| **Nature** | | |
| Implementation of the processing | | |
| Operations executed in processing | | Such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,  restriction, erasure or destruction. |
| Use cases | |  |
| Inventory of assets6 implementing processing | | Specifying:   * Human. * Organisational. * Materials. * Technicians/Information systems. |
| Data collection and generation | | |
| Data source | | External to the processing (other processing operations, controllers, or entities) or internal to the processing. |
| Inferred or generated data | | Categories of data inferred in relation to the purposes of processing. |
| Access to data | | |
| Categories of parties involved in the processing | | With regard to the phases of the processing, define the  categories of parties involved in the operations. |
| External parties and their roles | | Processors, sub-processors, developers, etc. Phases or stages of processing in which they are involved and the processing operations they are entrusted with by the controller, as well as the legal link with the controller. |
| Roles of access to the data of the intervening parties | | For each party, define their roles in relation to the identified processing operations. |
| Information flows with other processing operations of the controller | | It is necessary to take into account the organisation's processes related to processing (quality management, business intelligence, directories, agendas, etc.) in order to identify the relationship between the  processes with the organisation's processing in a single process/processing map. |
| Data disclosure | | Identification of the entities to which data are transferred, with their geographical locations, legal authorisations and safeguards established for such communication, as well as any other information  relevant to risk management. |
| Weaknesses | | |
| Relevant characteristics/constraints and risk factors of the technologies involved | |  |
| Vulnerabilities | | Derived from technical, but also human or organisational elements, which may lead to unauthorised access or loss of data quality,  accuracy, availability, resilience, etc. |
| Measures and safeguards implemented | | |
| Data Protection Policies |  | |
| Privacy and security measures and safeguards by default and from the design of the  processing | A set of legal, organisational, and technical safeguards incorporated in the processing irrespective of the level of risk that may be  associated with the processing. | |
| Privacy and security measures and safeguards adopted according to the risk. | A set of legal, organisational, and technical safeguards that are adopted according to the risk. This section could be empty in the first iteration of the risk management cycle. Depending on whether the risks are being addressed with different measures, this  section would be completed. | |
| Safeguards on international transfers | Contractual clauses, BCR's or other. | |
| **Context** | | |
| Sector of activity | | |
| Market or economic sector |  | |
| Regulatory framework | | |
| Regulatory framework for implementation | In addition to data protection regulations, the sectoral regulations applicable to the processing shall be taken into account. | |
| Standards, certification, codes of conduct applicable to the processing |  | |
| Possible side/unwanted effects of the processing | | |
| Derived from the scope and field |  | |
| Derived from the nature of the data |  | |
| Derived from the market or sector |  | |
| Other side effects of processing |  | |
| Data breaches | | |
| Known incidents in similar processing | Known incidents should be understood as both incidents in the organisation itself and incidents in other organisations with similar or identical technical, organisational, human, etc. means.  In this context, it may be helpful to consult the AEPD's security breaches microsite7. | |
| Potential threats | Derived from technical, human or organisational elements, as well as from specific situations or social contexts (economic crisis, pandemic, political or social instability, etc.) which, by exploiting a vulnerability of one of the identified assets, could give rise to breaches with undesired consequences for the rights and freedoms of  data subjects: | |

Table 11 Information derived from a High-Level Processing Analysis

3 In case of co-responsibility, determine these co-responsibilities and their limits.

4 Recital 33: It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

5 WP248 Guidelines

6 Asset is defined as any asset or resource that may be required to implement and maintain a processing activity throughout its life cycle, from conception and design to the end of the processing life.

7 <https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplnto/brechas-de-seguridad>

|  |  |
| --- | --- |
| Name of the phase: |  |
| Previous phases |  |
| Subsequent phases |  |
| Operation(s) carried out | Several operations could be executed in the same phase. |
| Assets implementing the operation | Assets as defined in the previous section. |
| Relevant features of the implementation phase | Implementation can be done with organisational measures and/or technical elements. Organisational measures may include aspects such as the physical layout of the premises (e.g. isolation of interview areas) or the generation and destruction of physical reports. On the other hand, in the case of technical components, disruptive technologies or novel use  of certain techniques, among others, could be identified. |
| Data processed |  |
| Inferred or generated data |  |
| Data source | External to the processing (other processing,  controllers, or entities) or internal to the processing. |
| Destination of data | External to the processing (other processing operations, controllers, or entities) or internal to the processing. |
| External actors, their roles, and functions | Processors, sub-processors, developers, etc. and in different functions: editor, support, etc  web, administrator, analysis, DB, marketing, etc. |
| Known incidents of implemented phases with similar characteristics,  their own or others |  |
| Vulnerabilities and threats | Derived from technical, but also human or organisational elements, which may result in unauthorised access or loss of |

|  |  |
| --- | --- |
|  | data quality, accuracy, availability, resilience, etc. |
| Privacy and security measures and safeguards by default | Set of legal, organisational, and technical safeguards already in place. |
| Privacy and security measures and safeguards adopted according to the risk | A set of legal, organisational, and technical safeguards that are adopted according to the risk. This section could be empty or have a first approximation in the first iteration of the risk management cycle. Depending on whether the risks are addressed with different  measures, this section would be completed. |

Table 12 Description of a Processing Phase

|  |  |
| --- | --- |
| **Asset:** | An asset identifier |
| Technologies involved: |  |
| Processing and phases in which it is used: | The same asset can be used in different processing |
| Processing operations where this is necessary: |  |
| Data that are processed: |  |
| Data that are generated: |  |
| Roles with access to the asset and their level of privilege: |  |
| Vulnerabilities (inherent to the asset) |  |
| Threats (internal and external) associated with the asset |  |

Table 13 Description of assets involved in processing

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood** | Very high | Medium | High | Very high | Very high |
| High | Low | High | Very high | Very high |
| Low | Low | Medium | High | Very high |
| Unlikely | Low | Low | Medium | Very high |
|  | | Very limited | Limited | Significant | Very significant |
| **Impact** | | | |

Table 14 Likelihood x Impact Matrix to determine the Level of Risk

|  |  |  |
| --- | --- | --- |
| **Level of impact** | **Description** | **Fundamental rights** |
| Very significant | It affects the exercise of fundamental rights and public freedoms established in the Constitution8, and its consequences are irreversible.  and/or  The consequences are related to special categories of data or to criminal offences and are irreversible.  and/or  It causes significant social harm, such as discrimination, and is irreversible  and/or  It affects particularly vulnerable data subjects, especially children, in an irreversible way.  and/or  Causes significant and irreversible moral or material losses. | Equality  Non-discrimination Life  Physical integrity Religious freedom Personal freedom  Personal and family privacy  Self-image Expression Information Academic  Meeting |
|  |  |
| Significant | The above cases when the effects are reversible.  and/or  Loss of control of the data subject over their personal data, where the extent of the data is high in relation to the categories of  data or the number of subjects. | Association  Free and equal access to public office and public functions |

8 The fundamental rights guaranteed by the Spanish Constitution are, among others, the right to equality and non-discrimination; the right to life and physical integrity, religious freedom, personal freedom, personal and family privacy and self-image, freedom of expression and information, academic freedom, freedom of assembly, freedom of association, free access to public positions and functions in conditions of equality, effective judicial protection, criminal law, education, trade union membership and the right to petition.

|  |  |  |
| --- | --- | --- |
|  | and/or  Identity theft of data subjects occurs or may occur | Effective judicial protection  Criminal legality |
| and/or | Education |
| Significant financial losses to data subjects may occur | Trade union membership |
| and/or | Right to petition |
| Loss of confidentiality of data subject to the duty of professional secrecy or breach of the duty of confidentiality |  |
| and/or |  |
| There is a social detriment to data subjects or certain groups of data subjects |  |
|  | Very limited loss of control of some personal data and to specific data subjects, other than special category or irreversible criminal offences or convictions |  |
|  | and/or |  |
| Limited | Negligible and irreversible financial losses |  |
|  | and/or |  |
|  | Loss of confidentiality of data subject to professional secrecy but not special categories or infringement  penalties |  |
| Very limited | In the above case, when all effects are reversible |  |

Table 15 Criteria for determining the Level of Impact

|  |  |
| --- | --- |
| **Likelihood** |  |
| Very high | If the risk factor is materialised and not likelihood-dependent, e.g. because the wp248 Guidelines identify the use of a technology as a risk and it is present in the processing.  and/or  Whether there is evidence of several materialisations of this risk in the last year in different entities.  and/or  Whether there is evidence of such a risk materialising in the last year in the same entity.  and/or  There are audits/studies that identify important vulnerabilities in organisational procedures or technical means linked to this risk. |
| High | Whether there is evidence of such a risk materialising in the last year in any entity.  and/or  Studies show that the likelihood could be high.  and/or  There are audits/studies that identify possible vulnerabilities in organisational procedures or technical means linked to this risk.  and/or  The elements linked to the risk factors have been implemented with non-mature technologies or organisational procedures, without following quality standards, without  being certified by independent third parties |
| Low | Whether there is evidence of such a risk materialising in the last 10 years in any entity. |
| Unlikely | If there is no evidence of such a risk materialising in any case. |

Table 16 Criteria for determining the Likelihood of Materialisation of a Risk Factor

|  |  |
| --- | --- |
| Operations related to the purposes of processing | Risk factors deriving from the purpose  stated of the processing and other purposes related to the main purpose. |
| Types of data used | Risk factors related to the scope of the processing that arise from data collected, processed or inferred in the  processing. |
| Extent and Scope of Processing | Risk factors related to the scope of the processing relating to the number of data subjects concerned, the diversity of data or aspects processed, the duration in time, the volume of data, the geographical extent, the exhaustiveness  on the person, frequency of collection, etc. |
| Categories of Data Subjects | Risk factors related to the scope of the processing related to the category of data subjects, such as employees, minors, elderly people, persons in a situation of  vulnerability, victims, disabled people, etc. |
| Technical Factors of Processing | | Risk factors that arise from the nature of the processing when implemented with certain technical characteristics or  technologies. |
| Data collection and generation | | Risk factors that arise from the  nature of the processing when data are specifically collected or generated. |
| Side Effects of Processing | | Risk factors that arise from the processing context as consequences may occur that are not foreseen in the  original intended purposes of the processing. |
| Category of controller/processor | | Context-related risk factors  specific to the sector of activity, business model or type of entity. |
| Data disclosure | | Risk factors that arise from the context in  which the data disclosures are made to third parties within the framework of the processing |
| Data breaches | | Risk factors that arise from the possible  materialisation of personal data breaches. |

Table 17 Categories of Risk Factors identified in the GDPR or in its development.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Profiling  E.g. and without being exhaustive:   * Profile creation * Use of profiles * Classification of individuals * Targeting products/services to individuals or groups * Behavioural analysis (assessment and rating of emotions, moods, habits, preferences, etc.) * Other | High |
| Assessment of subjects e.g. and without being exhaustive:   * Valuation * Score * Other | High |
| Prediction  E.g. and without being exhaustive:   * Inference of new personal data * Other | High |
| Employee control  E.g. and without being exhaustive:   * Employee assessment * Workplace observation * Workplace monitoring * Workplace image recording * Audio recording in the workplace * Image-based monitoring in the workplace * Sound-based monitoring in the workplace * Geolocation of workers en-route * Time spent performing tasks * E-mail monitoring and control * Monitoring and control of Internet browsing at the workplace * Monitoring the use of IT applications/services   in the workplace   * Telephone usage monitoring * Other | Medium |
| Internet access control e.g. and without being exhaustive:   * Analysis or evaluation of Internet usage times * Analysis or evaluation of Internet browsing activity * Analysis or evaluation of alarms about browsing to specific Internet sites * Analysis or evaluation of navigation alarms to   specific content on the Internet   * Other | Medium |
| Observation  E.g. and without being exhaustive:   * Image surveillance * Sound surveillance * Communications surveillance * Heat or other emissions surveillance * Transmission surveillance * Internet surveillance * Other | High |
| Monitoring  E.g. and without being exhaustive:   * IoT-based management * Image-based control | High |
| * Sound-based control * Communications control * Heat or other emissions control * Transmission control * Internet control * Geolocation-based control * Other |  |
| Supervision  E.g. and without being exhaustive:   * Control * Image-based analysis * Sound-based analysis * Communications analysis * Heat or other emissions analysis * Transmission analysis * Internet analysis * Geolocation-based analysis * Road traffic control * Other | High |
| Contact tracing | Very high |
| Physical access control e.g. and without being exhaustive:   * Workplace access control * Access control to commercial premises * Access control to events * Access control to sports facilities * Access control to buildings (public/private) * Other | Low |
| Location  E.g. and without being exhaustive:   * Geolocation * Mobility profiling * Determination of usual locations * Identification of frequent access sites * Data about the person inferred from geolocation * Other | Medium |
| Unique identification | Low |
| Automated decisions without human intervention | High |
| Automated processing for decision support  E.g. and without being exhaustive:   * DSS * Business intelligence that goes beyond purely statistical data * Data mining * Other | Medium |
| Deciding on or preventing the exercise of fundamental rights  E.g. and without being exhaustive:   * Right to equality | Very High |
| * Right to non-discrimination * Right to life and physical integrity * Right to freedom of religion * Right to personal liberty * Right to personal and family privacy * Right to self-image * Right of free speech and information * Right to academic freedom * Right to freedom of meeting * Right of freedom of association * Right to free and equal access to public office and public service * Right to effective judicial protection * Right to criminal legality * Right to education. * Right to trade union membership * Right to petition * Other rights or freedoms |  |
| Decide on the data subject's control of their personal data   * Right of access. * Right to rectification * Right to object * Right to erasure * Right to restriction of processing * The right not to be subject to automated decisions without human intervention. * Right to portability * Other | High |
| Deciding on access to a service | High |
| Deciding on the execution or performance of a contract | High |
| Deciding on access to financial services | High |
| Legal effects on persons | High |
| Assessment and/or prediction of disease/health potential genetically. | Very High |
| Preservation for storage purposes | Medium |

Table 18 Risk Factors associated with the Operations related to the Purposes of Processing.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Personal documents e.g. and without being exhaustive:   * Emails * Personal letters * Diaries * Notes on e-readers * Other | Medium |
| Information from vital activities logger applications | High |
| Personal aspects  E.g. and without being exhaustive:   * People or groups with whom they interact * Temperament * Character * Intelligence * Social roles * Adaptability * Risk tolerance * Audio-visual content tastes/preferences (interactive TV, content platforms, social networks, ...) * Health care * Cultural (reading, music, art, ...) * Membership and activities in social and cultural associations * Other | Medium |
| Consumption preferences, habits, tastes, needs, etc. that do not allow the inference of information related to special categories of data  E.g. and without being exhaustive:   * Consumption preferences: category of store, type of establishment; type of products; etc. * Consumption habits (customer loyalty cards,   web activity, ...)   * Preferences for audio-visual content in different media (interactive television, content platforms, social networks, ...) * Leisure preferences (sports, restaurants, museums, theatres, music, etc.) * Other | Medium |

|  |  |
| --- | --- |
| Job performance  E.g. without being exhaustive:   * Workplace access control * Recording images of the workstation * Audio recording at the workplace * Worker assessment by means of images captured from worker devices and displays * Sound-based worker assessment * Image recording in access areas or in offices * Audio recording in access areas or in offices. * Monitoring of employee equipment * Performance inference through indicators (productivity and quality of work, efficiency, training acquired, objectives achieved) * Other | Medium |
| Economic situation  E.g. without beingexhaustive:   * Personal income * Monthly income * Assets (movable/immovable) * Employment status * Other | Medium |
| Financial statement  E.g. without being exhaustive:   * Financial soundness * Debt capacity * Level of debt (personal loans, mortgages) * Solvency lists * Non-payments * Assets (investment funds, income generated, equities, receivables, income received, etc.) * Liabilities (expenditure on food, housing, education,   health, taxes, credit payments, credit cards or personal expenses, etc.; or debts or obligations   * Other | Medium |
| Data on payment methods:  E.g. and without being exhaustive:   * Credit cards * Information on access to virtual currency services. * Others. | High |
| Behavioural data  E.g. and without being exhaustive:   * Reliability of the person * Habits and values that facilitate coexistence * Habits and values that facilitate work and study * Habits and values that influence personal, occupational and family wellbeing * Habits and values influencing engagement with people and society * Job stability * Complaints about the person * Other | Medium |
| Location data  E.g. and without being exhaustive:   * Register of movement * Location-based register of routines * Register of usual places * Other | Medium |
| Highly personal data[[1]](#footnote-1) not included in rankings above | High |
| Health data  E.g. and without being exhaustive:   * Clinical records * Health reports * Health-related sick leave reports for the Occupational Risk Prevention Service * Prescriptions * Physical health data * Mental health data * Data relating to the provision of health care services * Health data from eHealth applications * Documents relating to the patient's care processes (including identification of doctors and other professionals involved) * Any information that is considered to be significant   for accurate and up-to-date knowledge of the patient's health status   * Other | Very High |
| Biometric data  E.g. and without being exhaustive:   * Fingerprint * Facial features * Iris * Veins in the palm of the hand * Voice * Ear * Gestures | High |

|  |  |
| --- | --- |
| * Gait pattern * Body descriptors of any kind * Other |  |
| Genetic data | Very High |
| Special categories of data or allowing inferences to be drawn from them e.g. and without being exhaustive:   * Ethnic origin * Racial origin * Political opinions * Religious convictions * Philosophical convictions * Trade union membership * Data relating to health * Data relating to sex life * Data relating to sexual orientations * Other | Very High |
| Special categories of pseudonymised data | High |
| Personal data relating to convictions and criminal offences | Very High |
| Metadata  E.g. and without being exhaustive:   * Electronic communications traffic data * Identification of sender and/or receiver in communications * Data on internet connections: location;   software and hardware characteristics of the device with which you are connected; social networks or pages in general to which you are logged in, connection (IP, service provider, download speed), ..   * Other | Medium |
| Unique identifiers  E.g. and without being exhaustive:   * IP address * MAC address * IMSI * IMEI * Device ID * Telephone No. * NIF, NIE, Passport N. or equivalent * Social Security No. * Vehicle registration number * Credit card number. * UIDs (unique user registration identifiers on websites) * Unique identifiers derived from the characteristics   of the device (e.g. access to the battery information of a device, advertising id of the device)   * Unique identifiers added to files (e.g.   metadata of photographs uploaded to social networks) | Medium |

|  |  |
| --- | --- |
| * Other |  |
| Electronic communications data and metadata and inferred electronic communications data  E.g. and without being exhaustive:   * Emails * Instant messaging * Telephone calls * Video calls * Other | Medium |
| Web browsing data  E.g. and without being exhaustive:   * Logging of visited pages (e.g. history of   browsing, web server logs, ...)   * Logging of the time spent on each page * Logging of the time of the visit to the site * Logging of the number of connections * Logging of mouse activity through the different parts of the website * Browser used * Other | Medium |

Table 19 Risk Factors associated with the Types of Data used in the Processing.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Systematic  E.g. and without being exhaustive:   * It is caused according to a system * It is pre-set, organised or methodical * It takes place as part of an overall data collection plan * It is carried out as part of a strategy * Other | High |
| Exhaustive on persons  E.g. and without being exhaustive   * A wide range of different elements are collected and dealt with * Multiple spheres of life * Different aspects of personality are covered * Other | High |
| Involves a large number of subjects e.g. and without being exhaustive:   * The number of data subjects concerned is high in   absolute numbers | Very High |

|  |  |
| --- | --- |
| * The number of data subjects concerned is high in relation to the relevant population * The number of data subjects is relevant in relation to the geographic extent * Other |  |
| The volume of data processed is very high | Very High |
| The duration of processing is high  E.g. and without being exhaustive   * The permanence of processing is high * Other | Medium |
| The processing activity has a wide geographical scope  E.g. and without being exhaustive:   * Regional, national or supranational level * Other | Medium |
| Large-scale processing E.g. and without being exhaustive   * Processing of data from patients in the regular   hospital operations   * Processing of the movement data of natural persons using the   public transport systems in a city (e.g. monitoring  through transport cards)   * Processing of real-time geolocation data of customers of an international fast food chain for statistical purposes by a processor specialised in the provision of such services * Processing of data from customers in the regular   business of an insurance company or a bank   * Processing of personal data for behavioural advertising by a search engine * Processing of data (content, traffic, location) by telephony or Internet service providers * Other | High |
| Excessive collection of data in relation to the purpose of the  processing | High |

Table 20 Risk Factors associated with the Extent and Scope of Processing.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Childs under 14 y.o. | Very High |
| Victims of gender-based violence | Very High |
| Children dependent on vulnerable subjects | Very High |
| Persons under guardianship and custody of victims of gender-based violence | Very High |
| Elderly people with some degree of disability | High |
| Elderly people | Medium |
| People with mental illness | Very High |
| Disabled | High |
| Persons who access social services | Medium |
| People at risk of social exclusion | High |
| Employees | Low |
| Asylum seekers | High |
| Patients | High |
| Vulnerable subjects  E.g. and without being exhaustive:   * In a situation of particular vulnerability * There is an imbalance between the position of the data subject and the controller * Other | Very High |

Table 21 Risk Factors associated with Data Subject Category.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Hospital information system | High |
| Interactive TV | Medium |
| Web services | Medium |
| Mobile applications | Medium |
| Location registration systems | High |
| Facial recognition | High |
| Fingerprint | High |
| Internet of Things (IoT) | Very High |
| Innovative use or new organisational solutions | High |
| Innovative use of established technologies E.g. and without being exhaustive:   * Technologies where no assessment has been made of the   impact on privacy   * Technologies used on a new scale * Other | High |
| Technologies combined with other technologies | Medium |
| New technologies  E.g. and without being exhaustive:   * Immature technologies * Emerging technologies * Other | High |
| High degree of fragmentation of the actors involved in the development and implementation of the  products/services implementing processing | High |
| Automated processing e.g. and not exhaustive:   * processing carried out by an automatic process without human intervention * Other | Medium |
| Intelligent System | Medium |
| Video surveillance | High |

Table 22 Risk Factors associated with Technical Processing Factors.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk factor** | | **Level of Risk** | |
| Access to credit reference database | | Medium | |
| Access to fraud database | | Medium | |
| Access to money laundering/terrorist financing database | | High | |
| Personal data obtained in publicly accessible areas e.g. and without being exhaustive:   * Motorway * Shopping centre * Street * Station * Market * Library * Other | | Medium | |
| Collection of data from public social media | | Low | |
| Collection of data from communications networks. | | Medium | |
| Collection of data from applications | | Medium | |
| Data from two or more processing operations for different purposes | | Medium | |
| Data from two or more different controllers | | Medium | |
| Association of datasets | | Medium | |
| Combination of datasets  E.g., and without being exhaustive:   * Cross-referencing of databases * Sensor data fusion * Other | | High | |
| Linking of database records of two or more processing operations for different purposes or by different controllers | Medium | |
| Collection of data by a controller other than the one processing and applying information exception 14.5 (b, c, d) | Medium | |
| Lack of transparency of the precise timing of data collection.  E.g. and without being exhaustive:   * Mobile systems * IoT * Domestic assistants * Connected cars * Others. | High | |
| New forms of data collection with risks for rights and freedoms | High | |

Table 23 Risk Factors associated with Data Collection and Generation.

|  |  |  |
| --- | --- | --- |
| **Risk Factor** | **Impact** | **Likelihood** |
| Exceeds the data subject's expectations e.g. and without being exhaustive:   * Excessive exposure of the data subject * Segmentation that exceeds reasonable expectations * Inference of interest or other   characteristics based on non-obvious data and resulting in a profiling of the subject   * Other | Medium |  |
| Possible unauthorised reversal of pseudonymisation | Very High |  |
| Possible loss of control by the controller over the data processed by the processor. | High |  |
| It could determine the financial situation | Medium |  |
| It could determine the capital solvency | Medium |  |
| It could deduce information related to special categories of data | High |  |
| May deprive data subjects of their rights and freedoms | Very High |  |
| May prevent control over their personal data | Very High |  |
| May lead to exclusion | High |  |
| May lead to discrimination | Very High |  |
| Possible identity theft | Very High |  |
| Possible fraud | Very High |  |
| Possible reputational damage | Very High |  |
| Possible Significant Economic Injury | Very High |  |
| Possible significant moral harm | Very High |  |
| Potential for significant social harm | Very High |  |
| Possible loss of confidentiality of data subject to professional secrecy | Very High |  |
| May prevent the exercise of a right | High |  |
| May prevent access to a service | High |  |
| May prevent access to a contract | High |  |
| It may collect personal data other than from service users.  E.g. and without being exhaustive:   * Home IoT * Smart speakers * Connected cars * Other | High |  |
| Possible manipulation of persons E.g. and without being exhaustive:   * Influencing behaviour and   decisions of individuals.   * Undermine their autonomy and individual freedom. * Generate disinformation. * Focalisation affecting access to pluralistic information * Filter bubble * Information overload * Other | High |  |
| Possibility of self-censorship | High |  |
| Possibility of bringing about a cultural change to surrender rights and freedoms | High |  |
| Unforeseen or unintended uses that could affect fundamental rights. | High |  |

Table 24 Risk Factors associated with Processing Side Effects.

|  |  |
| --- | --- |
| **Risk** | **Level of Risk** |
| Information company | Medium |
| Biotechnology company | High |
| Marketing company | Medium |
| Hospitals | High |
| Private researchers | Medium |
| Credit reporting institution | Medium |
| Fraud assessment institution | Medium |
| Financial institution | Medium |
| Employer | Low |
| Research projects | Low |
| Clinical test | High |

Table 25 Risk Factors associated with Category of Controller/Processor.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Regular transfer to states or organisations in  other countries without an adequate level of protection | Very High |
| Lack of transparency of the actors involved in the processing process  E.g. and without being exhaustive:   * Some types of social networks, * Types of digital marketing networks, * Types of blockchain-based processing, * Types of remote continuous learning AI. * Other | Medium |
| Free dissemination of unique identifiers.  E.g. and without being exhaustive:   * RFID Tags * SSIDs * MACs * Public keys * Others. | High |

Table 26 Risk Factors associated with Data Disclosure.

|  |  |
| --- | --- |
| **Processing** | **Scenario N** |
| Data breach materialised | Description of the type of breach. |
| Compromised data | List of data compromised in the breach. |
| Damage to the data subject | Detail what damage could be caused to the rights and freedoms of the data subject and, in general, to their interests.  Also defining the extent in data subjects. |

Table 27 Description of a Personal Data Breach Scenario.

|  |  |
| --- | --- |
| **Size of the breach** | **Impact on Rights and Freedoms** |
| Confidentiality | Maximum / High / Medium / Low |
| Integrity | Maximum / High / Medium / Low |
| Availability | Maximum / High / Medium / Low |
| Traceability | Maximum / High / Medium / Low |
| Authenticity/Identity | Maximum / High / Medium / Low |
| Resilience | Maximum / High / Medium / Low |
| Data breaches in measures and in technical and organizational safeguards of data protection | Maximum / High / Medium / Low |
| Errors in technical data processing operations | Maximum / High / Medium / Low |

Table 28 Compilation of Impact Level for cases of Personal Data Breaches.

|  |  |  |
| --- | --- | --- |
| **Size of the data breach** | | **Likelihood of materialisation** |
| Confidentiality | | Maximum / High / Medium / Unlikely |
| Integrity | | Maximum / High / Medium / Unlikely |
| Availability | | Maximum / High / Medium / Unlikely |
| Traceability | Maximum / High / Medium / Unlikely | |
| Authenticity/Identity | Maximum / High / Medium / Unlikely | |
| Resilience | Maximum / High / Medium / Unlikely | |
| Breaches in measures and in technical and organizational safeguards of data protection | Maximum / High / Medium / Unlikely | |
| Errors in data processing operations | Maximum / High / Medium / Unlikely | |

Table 29 Compilation of Likelihood of Personal Data Breaches Materialising.

|  |  |  |  |
| --- | --- | --- | --- |
| **Likelihood Today** | **Evolution of Likelihood** | | |
| Maximum | Maximum | Maximum | Maximum |
| High | High | Maximum | Maximum |
| Medium | Medium | High | Maximum |
| Low | Low | Medium | High |
|  | Short-Term  < 1 year | Medium-Term  < 5 years | Long-Term Longer than 5 years |

Table 30 Evolution of the Likelihood of a data breach materialising over time

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dimension: C/A/I/T/AU/R/F/E** | | | | | |
| **Likelihood** | Very high | Medium | High | Very high | Very high |
| High | Low | High | Very high | Very high |
| Low | Low | Medium | High | Very high |
| Unlikely | Low | Low | Medium | Very high |
|  | | Very limited | Limited | Significant | Very significant |
| **Impact** | | | |

Table 31 Likelihood x Impact Matrix to determine the Level of Risk of a Personal Data Breach

|  |  |  |
| --- | --- | --- |
| Small Breach | < Impact | > Likelihood |
| Large Breach | > Impact | < Likelihood |

Table 32 Possible Relationship between Impact and Likelihood on data breaches subject to the Volume of Data.

|  |  |  |
| --- | --- | --- |
| **Dimension:** | **C/A/I/T/AU/R/F/E** |  |
| **Assets** | **Likelihood** | **Impact** |
| Active 1 | Likelihood of materialisation | Level of impact in terms of how a total or partial loss of the asset in dimension C/A/I/T/AU/R/F/E could affect the  rights and freedoms of data subjects. |
| … | … | … |
| Asset N | … | … |

Table 33 Analysis of the Assets involved in the Processing.

|  |  |  |
| --- | --- | --- |
| **Risk factor** | **Impact** | **Likelihood** |
| **Internal context of the organisation** |  |  |
| Lack of maturity in the organisation's governance and processes |  |  |
| Internal organisational crisis |  |  |
| Existence of other high-risk processing in the organisation |  |  |
| Acting as a processor for numerous (hundreds or thousands) of controllers |  |  |
| Other |  |  |
| **Operations related to the purposes** |  |  |
| There is frequent and repeated contact with  data subjects in a manner that may be intrusive to the privacy of the data subject |  |  |
| There is a real likelihood that the data will be processed in the future for purposes other than those envisaged at the time of collection, in particular if these purposes are more intrusive or exceed the expectations of the  data subjects |  |  |
| Moulding or presentation of the digital reality based on a profile |  |  |
| Nudging or positive reinforcement to influence behaviour by exploiting cognitive biases or psychological weaknesses |  |  |
| Other |  |  |
| **Extent and Scope of Processing** |  |  |
| processing involves a large number of actors and/or organisations and may represent a risk of loss of control of the  personal data |  |  |
| Other |  |  |
| **Technical Factors of Processing** |  |  |
| Educational platforms |  |  |
| Internet of Bodies/Wearables |  |  |
| Neurological interfaces |  |  |
| Artificial Intelligence |  |  |
| Blockchain |  |  |
| Other |  |  |
| **Category of controller/processor10** |  |  |
| Public bodies and public administrations |  |  |
| Teaching and education centres |  |  |
| Insurance company |  |  |
| Other |  |  |
| **Data collection and generation** |  |  |
| False positive rates |  |  |
| False negative rates |  |  |
| Other |  |  |
| **Side effects** |  |  |
| Possible inference of special categories of data from the accumulated information from the  user |  |  |
| Affects or is likely to affect the best interests of the minor |  |  |
| Discrimination in the offer of options, products or services due to user profiling |  |  |
| Limitation of the freedom of autonomy |  |  |
| Decision-making biases |  |  |
| Algorithmic discrimination |  |  |
| Cultural aspects affecting perception of intrusion or interpretation of data |  |  |
| Other |  |  |
| **Data disclosure** |  |  |
| Timely transfer to states or organisations  in other countries without an adequate level of protection |  |  |
| **Other** |  |  |
| Those foreseen in the codes of conduct to which the entity adheres |  |  |
| Foreseen in the certification schemes |  |  |
| Any other risk factor |  |  |

Table 34 Examples of other Possible Risk Factors

10 In relation, generally, to non-supporting processes.

|  |  |
| --- | --- |
| **Risk factor** | **Level of Risk** |
| Breakdown of the rule of law |  |
| Radical alteration of legal safeguards |  |
| Geostrategic changes |  |
| Disruptive technological advances |  |
| National emergencies |  |
| Other |  |

Table 35 Examples of High-Impact Cases

|  |  |
| --- | --- |
| **As for nature:** | |
|  | Change, rearrange or reorganise the phases of processing. |
|  | Eliminate some phase of processing. |
|  | Isolate and segregate processing steps from each other so that they process data in a more limited way. For example, by ensuring that some steps do not process personal data (e.g. anonymised data) or by using  their pseudonymisation. |
|  | Review data processing procedures. |
|  | Change technical choices to implement  processing operations by less invasive and/or more mature technologies. |
|  | Switch, in the above sense, to technologies that are more reliable from a data protection point of view, by using  for example, the use of PETs (Privacy Enhanced Technologies). |
|  | Replace automated processing with manual processing incorporating monitoring and control procedures. |
|  | Carrying out human supervision of automated decisions  . |
|  | Use specially qualified personnel at certain stages of processing, especially in their supervision. |
|  | Redesign the procedures for collecting, enriching or generating personal data. |
|  | Reorganise the physical spaces where processing is carried out. |
|  | Redesign the orientation of work towards local, online or teleworking. |
|  | Check the possibility of implementing alternative means of processing: automatic/manual, different automation options,… |
|  | Limit access to personal data that is required to be held in the system under the management of processors. |
|  | Others. |
| **As for scope:** | |
|  | Target processing to a smaller number of subjects. |
|  | Focus processing on covering fewer areas of the subject's life. |
|  | Target processing to a limited geographical area. |
|  | Limit the number of interveners or participants. |
|  | Limit, in the design of the processing, the amount of time which the processing uses data of the same subjects. |
|  | Limit the degree to which the processing interacts or is linked to other processing of the same entity. |
|  | Limiting the extension of processing to subjects considered vulnerable (the elderly, child, handicapped, etc.) |
|  | Define, within the processing, concrete use cases with disjoint scopes. |
|  | Others. |
| **As for context:** | |
|  | Define the social or economic contexts in which the processing will be applied. |
|  | Define restrictive use cases targeted at specific sectors. |
|  | Select processors to minimise legal, social or political risks. |
|  | Limit links or relationships with other controllers' processing11. |
|  | Others. |
| **As for purposes:** | |
|  | Limit or redefine the purposes of processing. |
|  | Eliminate secondary purposes in processing. |
|  | Define, within the processing, specific use cases for independent purposes. |
|  | Others. |

Table 36 Examples of Possible Measures on the Processing Concept

11 For example, when customer tracking processes in shopping centres are supported by the same service that supports different managers with a technology that allows linking the activity of the same person.

|  |  |
| --- | --- |
| **As for the governance framework:** | |
|  | There is a specific mandate and commitment from the organisation's management regarding the management of risk to the rights and freedoms of the data subjects. |
|  | Risk management for the rights and freedoms of data subjects is integrated into the organisation's management processes. |
|  | There is an explicit reference to the risk management policy for rights and freedoms in the organisation's risk management framework. |
|  | Measures implementing risk management policies for rights and freedoms are differentiated from policies for managing compliance risk, legal risk or civil and criminal liability risk. |
|  | The roles and allocation of responsibilities and resources necessary to ensure data protection in the organisation are defined. |
|  | The necessary resources are in place to ensure data protection in the organisation. |
|  | The cycle of continuous improvement is in place to ensure that data protection policies are effective and appropriate to the nature, context, scope and purposes of the various processing operations throughout its life cycle. |
|  | There are tangible indicators on the effective implementation of data protection policies. |
| **As for data protection advice:** | |
|  | The DPO has been appointed or the collegiate body has been defined;this will exercise the functions of the DPO in the organisation (Articles 37, 38 and 39 GDPR) even though it is not mandatory12. |
|  | The involvement of the DPO in the procedures for deciding and defining processing operations is established. |
|  | Internal channels for communication with the DPO are defined, as well as the data protection advice and/or those responsible for managing risks to rights and freedoms. |
|  | Actions have been implemented so that the members of the organisation are aware of the role of the DPO, the data protection advisor and/or the person responsible for the management of risks to the rights and freedoms of their functions and the channels for communicating with them. |
|  | The advisory and supervisory duties (Art. 39.1.a and b) of the DPO or the data protection advisor extend to the development, maintenance and surpervision of data protection policies. |
|  | Others. |

12 Where the appointment of a DPO is mandatory, this appointment is not subject to the outcome or need arising from risk management.

|  |  |
| --- | --- |
| **As for data protection policies embedded in procedures:** | |
|  | Active accountability strategies for data protection are included in the procedures for the conception, design and implementation of new processing operations: risk management for rights and freedoms, data protection by design, data protection by default, transparency of processing and security by design, and by default. |
|  | Included in the procurement procedures for products, systems or services that are to implement operations within the processing activity are the requirement for information and guarantees13 to ensure and be able to demonstrate that such processing complies with the GDPR. |
|  | The points of contact within the organisation for each processing of personal data are designated. |
|  | The complaint boxes implement the management of abuses in the areas of data protection. |
|  | Data protection is integrated into the working procedures at local, remote and teleworking. |
|  | There is a BYOD policy that integrates data protection requirements. |
|  | The processing management policy includes the conditions for the verification and processing of risk management for rights and freedoms. |
|  | Expiry clauses in the processing conditions are set out in the processing management policy. |
|  | Others. |
| **As for the attention to data subjects14** | |
|  | To the extent that they can result in a decrease in risk, provide procedures for addressing entitlements that go beyond the minimums set out in Chapter III of the GDPR. |
|  | To the extent that they can result in a decrease in risk, have transparency policies that go beyond the minimums set outin Chapter III of the GDPR98. |
|  | To have channels of communication with data subjects in relation to the privacy protection. |
|  | There are procedures for consultation with data subjects regarding the protection of their rights. |
|  | Other |

13 These can be of various types: independent audits, certifications or others; whether at technical, compliance, procedural or other levels.

14 Remember that data subjects are not only customers, but also stakeholders, to the extent that their personal data are processed, employees, other natural persons with whom the entity has a relationship and any other person indirectly affected by the processing.

15 These transparency policies will be specified in each processing operation as data protection strategies by design.

|  |  |
| --- | --- |
| **In relation to security (both organisational and information security):** | |
|  | A reference to the management of the risk to rights and freedoms in the security policy applicable to the processing of personal data, as well as in the general security policy applicable to the organisation. |
|  | An integration of the protection of rights and freedoms into the information security management system (ISMS). |
|  | A correct differentiation of roles between the DPO and those responsible for IT or information security. |
|  | An implementation of the necessary coordination between the DPO and the security officer of the organisation, the information system and others depending on the entity. |
|  | A clear definition of the scope of the DPO's participation in safety committees. |
|  | Others. |
| **As for legal guarantees:** | |
|  | Confidentiality commitments are established for those who have access to personal data. |
|  | Establishment of guarantees for processors that go beyond the provisions of Article 28 of the GDPR. |
|  | Commitments are in place not to engage in efforts that could lead to the reidentification of individuals in disassociated datasets. |
|  | Legally valid instruments are in place to protect the rights and freedoms of data subjects in the event of the materialisation of specific risks. |
|  | Legally valid instruments are available to compensate in a balanced manner the data subjects (not the controller) for damage to their rights and freedoms in the event of the materialisation of specific risks. |
|  | Others. |
| **As for the training and preparation of personnel in relation to data protection:** | |
|  | Awareness and training measures are in place for personnel involved in the definition or conception of new processing |
|  | Establishment of awareness-raising and training measures for personnel involved in personal data processing operations. |
|  | Guides for workers, according to their specific roles, include information related to the obligations on data protection. |
|  | Guides for workers, according to their specific roles, include information on how to deal with complaints relating to rights. |
|  | Guides for workers, according to their specific roles, include information on what to do in the event of a personal data breach. |

|  |  |
| --- | --- |
|  | Guides for workers, according to their specific roles include information regarding their rights and channels of complaint on data protection issues. |
|  | Others. |
| **As for the relationship between the controller and the processor** | |
|  | Model contracts include reference to clauses applicable to the relationship between the controller and the processor. |
|  | The obligations of Article 28 of the GDPR are included in the procedures for hiring processors. |
|  | The procedures for hiring processors include detailed procedures for assessing the processor that will ensure that only a processor will be chosen who offers sufficient guarantees to implement appropriate technical and organisational measures in accordance with the risk of the Processing16. |
|  | Contractual clauses shall extend beyond the requirements set out in Article 28 of the GDPR for appropriate risk management of the processing17. |
|  | Contractual clauses include elements that can help the processor to understand the risks to the rights and freedoms of the data resulting from the processing18. |
|  | The contractual clauses cover the security measures applicable to the processing. |
|  | The contractual clauses include the obligation of the processor to obtain the approval of the controller prior to carrying out any change on security measures19. |
|  | The contractual clauses provide for the obligation of the controller to review these measures periodically on a risk-based basis20. |
|  | Additional steps to ensure compliance with personal data regulations are included in the procurement procedures. |
|  | The controller carries out its own audits of the processors in relation to the processing. |
|  | Independent third parties audit or certify the processor in relation to the processing. |
|  | Others. |
| **As for data disclosure:** | |
|  | Mechanisms are in place to have traceability of disclosure of personal data carried out by the controller and processor to processors, sub-processors and third parties. |
|  | There are procedures with the definition of mechanisms, safeguards and limits applicable to international data transfers for each processing operation. |

16 "94. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment" Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

17 Paragraph 112 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

18 Paragraph 110 and 131 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

19 Paragraph 123 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

20 Paragraph 123 of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

|  |  |
| --- | --- |
|  | There are procedures that reference to the binding corporate rules that would apply to the organisation, with details of the specific areas and processing applicable, as well as their limits. |
|  | Others. |
| **Within the document management policy:** | |
|  | There is a definition of documents that enable the controller to demonstrate compliance |
|  | Includes management process of the risks posed to rights and freedoms. |
|  | There is traceability and version control of the risk management documentation for the rights and freedoms that are generated. |
|  | Others. |
| **In relation to the procedures for the management of personal data breaches and processing incidents:** | |
|  | Procedures are defined to detect data breaches, incidents or errors in the processing of personal data. |
|  | The role of the DPO is clearly defined in the procedures relating to the management of personal data breaches, ensuring, at least, that it complies with 39.1. |
|  | There are defined procedures in place to react swiftly, at the organisational level, to breaches, incidents or errors in the processing of personal data. |
|  | Channels of communication, information and consultation on data breaches and incidents are defined with the parties involved in the processing of personal data. |
|  | Measures are defined to identify, in the data subjects' own communications to the controller/processor, information on breaches, incidents or errors. |
|  | There are procedures for the notification of personal data breaches to  the Supervisory Authority. |
|  | There are procedures for communicating personal data breaches to data subjects. |
|  | Specific scenarios of potential data breaches, errors or particularly serious incidents have been identified and the way to manage them has been defined,specifically, to protect the rights and freedoms of data subjects. |
|  | There is a link between the procedures for the management of breaches and incidents in the processing and risk management process, including the management of associated controls. |
|  | Others. |
| **As for the depth of risk management:** | |
|  | Carrying out an DPIA even if it is not mandatory. |
|  | There are internal procedures in place that make it necessary to carry out a DPIA regardless of whether or not there is a legal obligation to do so. |
|  | Others. |

|  |  |
| --- | --- |
| **Regarding monitoring and verification activities of governance measures:** | |
|  | Internal or external audit plans are in place to assess compliance with data protection policies. |
|  | Data protection certification policies are in place. |
|  | Where appropriate, mechanisms for adherence to codes of conduct are identified  . |
|  | Mechanisms, rules and procedures are in place to detect changes in the nature, scope, context or purposes of processing. |
|  | Decision mechanisms are in place so that, depending on previous changes or detected incidences, a new cycle of  risk review is carried out. |
|  | Others. |

Table 37 Examples of possible Data Protection Policies and Governance Measures

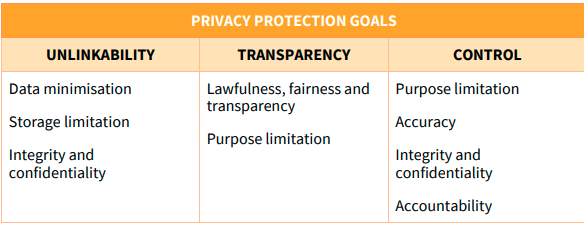


Table 38 Objectives of Privacy Protection “by Design”.

|  |  |  |  |
| --- | --- | --- | --- |
| **PRIVACY DESIGN STRATEGY** | | **DESCRIPTION AND TACTICS** | **DESIGN CONTROLS AND PATTERNS** |
| **Data oriented strategies** | Minimise | Avoid unnecessary processing of personal data. | Anonymisation Pseudonymisation |

|  |  |  |  |
| --- | --- | --- | --- |
| **PRIVACY DESIGN STRATEGY** | | **DESCRIPTION AND TACTICS** | **DESIGN CONTROLS AND PATTERNS** |
|  |  | TACTICS: **select**, **exclude**, **strip** and **destroy** | Block correlation in identity management systems federated  Data and metadata entry debugging |
| Hide | Limit the exposure of personal data.  TACTICS: **restrict**, **obfuscate**, **dissociate** and **mix**) | Access control.  Selective anonymisation of access to personal data sets.  Encryption  Homomorphic encryption Mixed networks  Attribute Based Credentials  Models of  zero knowledge (ZKP) |
| Separate | Keep personal datasets separate.  TACTICS: **isolate** and  **distribute** | Anonymous black lists  Physical and logical separation  Data unlinking techniques |
| Abstract | Limit the level of detail used in personal data processing as much as possible.  TACTICS: **summarise**, **group** and **perturb** | Aggregation over time K-anonymity  Noise added through obfuscation techniques  Dynamic granularity. Differential privacy |
| **Process oriented strategies** | Inform | Provide extended information of the processing.  TACTICS: **supply**, **explain** and **notify** | Privacy icons  Processing alerts.  Publish information on processing performance. |

|  |  |  |  |
| --- | --- | --- | --- |
| **PRIVACY DESIGN STRATEGY** | | **DESCRIPTION AND TACTICS** | **DESIGN CONTROLS AND PATTERNS** |
|  |  |  | Publish details of processing limitations and consequences.  Publish information  related to risk analysis. |
|  | Control | Provide data subjects with effective control over their personal data.  TACTICS: **consent**, **alert**, **choose**, **update**, **retract** | PIMS (personal information management systems)  Privacy preferences dashboard  Active broadcast of presence  Credential selection |
| Enforce | Application of the entity's data protection policies to the processing.  TACTICS: **create**, **maintain**, **uphold** | Apply data protection policies to the processing lifecycle. |
| Demonstrate | Be able to demonstrate that processing have been carried out in accordance with the entity's policies.  TACTICS: **record**, **audit** and **report**. | Audit of the processing  Recording and documentary control of the processing. |

Table 39 Data Protection Strategies, Description, Tactics, Controls and Patterns by Design.

|  |  |
| --- | --- |
| **Level of risk posed to rights and freedoms.** | **ENS Category** |
| Very High | High |
| High | High |
| Medium | Medium |
| Low | Low |

Table 40 Correspondence between the Level of Risk to Rights and Freedoms and category of the National Security Framework

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dimension** | Level | | | **SECURITY MEASURES** | |
|  | **B** | **M** | **A** |
|  |  |  |  | **org** | **Organisational framework** |
| All | applicable | = | = | [[org.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1075.htm#org.1) | Security Policy |
| All | applicable | = | = | [[org.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1076.htm#org.2) | Security Regulations |
| All | applicable | = | = | [[org.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1077.htm#org.3) | Security Procedures |
| All | applicable | = | = | [[org.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1078.htm#org.4) | Authorisation process |
|  |  |  |  | **op** | **Operational framework** |
|  |  |  |  | [[op.pl]](https://www.ccn-cert.cni.es/publico/ens/ens/1080.htm#op.pl) | Planning |
| All | applicable | + | ++ | [[op.pl.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1081.htm#op.pl.1) | Risk analysis |
| All | applicable | + | ++ | [[op.pl.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1082.htm#op.pl.2) | Security Architecture |
| All | applicable | = | = | [[op.pl.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1083.htm#op.pl.3) | Procurement of new components |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D | n.a. | applicable | = | [[op.pl.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1084.htm#op.pl.4) | Dimensioning / Capacity Management |
| All | n.a. | n.a. | applicable | [[op.pl.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1085.htm#op.pl.5) | Certified components |
|  |  |  |  | [[op.acc]](https://www.ccn-cert.cni.es/publico/ens/ens/1086.htm#op.acc) | Access control. |
| A T | applicable | = | = | [[op.acc.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1087.htm#op.acc.1) | Identification |
| I C A T | applicable | = | = | [[op.acc.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1088.htm#op.acc.2) | Access Requirements |
| I C A T | n.a. | applicable | = | [[op.acc.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1089.htm#op.acc.3) | Segregation of duties and tasks |
| I C A T | applicable | = | = | [[op.acc.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1090.htm#op.acc.4) | Access rights management process |
| I C A T | applicable | + | ++ | [[op.acc.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1091.htm#op.acc.5) | Authentication mechanism |
| I C A T | applicable | + | ++ | [[op.acc.6]](https://www.ccn-cert.cni.es/publico/ens/ens/1092.htm#op.acc.6) | Local access (local logon) |
| I C A T | applicable | + | = | [[op.acc.7]](https://www.ccn-cert.cni.es/publico/ens/ens/1093.htm#op.acc.7) | Remote login |
|  |  |  |  | [[op.exp]](https://www.ccn-cert.cni.es/publico/ens/ens/1094.htm#op.exp) | Exploitation |
| All | applicable | = | = | [[op.exp.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1095.htm#op.exp.1) | Inventory of assets |
| All | applicable | = | = | [[op.exp.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1096.htm#op.exp.2) | Security Settings |
| All | n.a. | applicable | = | [[op.exp.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1097.htm#op.exp.3) | Configuration Management |
| All | applicable | = | = | [[op.exp.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1098.htm#op.exp.4) | Maintenance |
| All | n.a. | applicable | = | [[op.exp.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1099.htm#op.exp.5) | Change Management |
| All | applicable | = | = | [[op.exp.6]](https://www.ccn-cert.cni.es/publico/ens/ens/1100.htm#op.exp.6) | Protection against malicious code |
| All | applicable | = | = | [[op.exp.7]](https://www.ccn-cert.cni.es/publico/ens/ens/1101.htm#op.exp.7) | Incident management |
| T | applicable | + | ++ | [[op.exp.8]](https://www.ccn-cert.cni.es/publico/ens/ens/1102.htm#op.exp.8) | Records of user activities |
| All | applicable | = | = | [[op.exp.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1103.htm#op.exp.9) | Incident management log |
| T | n.a. | n.a. | applicable | [[op.exp.10]](https://www.ccn-cert.cni.es/publico/ens/ens/1104.htm#op.exp.10) | Protection of activity records |
| All | applicable | + | = | [[op.exp.11]](https://www.ccn-cert.cni.es/publico/ens/ens/1105.htm#op.exp.11) | Cryptographic key protection |
|  |  |  |  | [[op.ext]](https://www.ccn-cert.cni.es/publico/ens/ens/1106.htm#op.ext) | External services |
| All | n.a. | applicable | = | [[op.ext.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1107.htm#op.ext.1) | Contracting and service level agreements |
| All | n.a. | applicable | = | [[op.ext.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1108.htm#op.ext.2) | Daily management |
| D | n.a. | n.a. | applicable | [[op.ext.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1109.htm#op.ext.9) | Alternative media |
|  |  |  |  | [[op.cont.]](https://www.ccn-cert.cni.es/publico/ens/ens/1110.htm#op.cont) | Continuity of service |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D | n.a. | applicable | = | [[op.cont.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1111.htm#op.cont.1) | Impact analysis |
| D | n.a. | n.a. | applicable | [[op.cont.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1112.htm#op.cont.2) | Continuity Plan |
| D | n.a. | n.a. | applicable | [[op.cont.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1113.htm#op.cont.3) | Periodic testing |
|  |  |  |  | [[op.mon]](https://www.ccn-cert.cni.es/publico/ens/ens/1114.htm#op.mon) | System monitoring |
| All | n.a. | applicable | = | [[op.mon.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1115.htm#op.mon.1) | Intrusion detection |
| All | applicable | + | ++ | [[op.mon.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1116.htm#op.mon.2) | Metrics system |
|  |  |  |  | **mp** | **Protection Measures** |
|  |  |  |  | [[mp.if]](https://www.ccn-cert.cni.es/publico/ens/ens/1118.htm#mp.if) | Protection of installations and infrastructure |
| All | applicable | = | = | [[mp.if.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1119.htm#mp.if.1) | Separate and access-controlled areas |
| All | applicable | = | = | [[mp.if.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1120.htm#mp.if.2) | Identification of persons |
| All | applicable | = | = | [[mp.if.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1121.htm#mp.if.3) | Fitting out the premises |
| D | applicable | + | = | [[mp.if.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1122.htm#mp.if.4) | Electric power |
| D | applicable | = | = | [[mp.if.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1123.htm#mp.if.5) | Fire protection |
| D | n.a. | applicable | = | [[mp.if.6]](https://www.ccn-cert.cni.es/publico/ens/ens/1124.htm#mp.if.6) | Flood protection |
| All | applicable | = | = | [[mp.if.7]](https://www.ccn-cert.cni.es/publico/ens/ens/1125.htm#mp.if.7) | Check-in and check-out of equipment |
| D | n.a. | n.a. | applicable | [[mp.if.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1126.htm#mp.if.9) | Alternative facilities |
|  |  |  |  | [[mp.per]](https://www.ccn-cert.cni.es/publico/ens/ens/1127.htm#mp.per) | Personnel management |
| All | applicable | = | = | [[mp.per.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1128.htm#mp.per.1) | Job characterisation |
| All | applicable | = | = | [[mp.per.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1129.htm#mp.per.2) | Duties and obligations |
| All | applicable | = | = | [[mp.per.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1130.htm#mp.per.3) | Awareness-raising |
| All | applicable | = | = | [[mp.per.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1131.htm#mp.per.4) | Training. |
| D | n.a. | n.a. | applicable | [[mp.per.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1132.htm#mp.per.9) | Alternative personnel |
|  |  |  |  | [[mp.eq]](https://www.ccn-cert.cni.es/publico/ens/ens/1133.htm#mp.eq) | Protection of equipment |
| All | applicable | + | = | [[mp.eq.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1134.htm#mp.eq.1) | Uncluttered workstation |
| A | n.a. | applicable | + | [[mp.eq.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1135.htm#mp.eq.2) | Workplace blocking |
| All | applicable | = | + | [[mp.eq.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1136.htm#mp.eq.3) | Protection of portable equipment |
| D | n.a. | applicable | = | [[mp.eq.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1137.htm#mp.eq.9) | Alternative media |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | [[mp.com]](https://www.ccn-cert.cni.es/publico/ens/ens/1138.htm#mp.com) | Protection of communications |
| All | applicable | = | + | [[mp.com.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1139.htm#mp.com.1) | Secure perimeter |
| C | n.a. | applicable | + | [[mp.com.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1140.htm#mp.com.2) | Confidentiality protection |
| I A | applicable | + | ++ | [[mp.com.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1141.htm#mp.com.3) | Protection of authenticity and integrity |
| All | n.a. | n.a. | applicable | [[mp.com.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1142.htm#mp.com.4) | Segregation of networks |
| D | n.a. | n.a. | applicable | [[mp.com.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1143.htm#mp.com.9) | Alternative media |
|  |  |  |  | [[mp.si]](https://www.ccn-cert.cni.es/publico/ens/ens/1144.htm#mp.si) | Protection of information media |
| C | applicable | = | = | [[mp.si.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1145.htm#mp.si.1) | Tagged |
| I C | n.a. | applicable | + | [[mp.si.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1146.htm#mp.si.2) | Cryptography |
| All | applicable | = | = | [[mp.si.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1147.htm#mp.si.3) | Custody |
| All | applicable | = | = | [[mp.si.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1148.htm#mp.si.4) | Transport: |
| C | applicable | + | = | [[mp.si.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1149.htm#mp.si.5) | Deletion and destruction |
|  |  |  |  | [[mp.sw]](https://www.ccn-cert.cni.es/publico/ens/ens/1150.htm#mp.sw) | Protection of software |
| All | n.a. | applicable | = | [[mp.sw.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1151.htm#mp.sw.1) | Development |
| All | applicable | + | ++ | [[mp.sw.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1152.htm#mp.sw.2) | Acceptance and commissioning |
|  |  |  |  | [[mp.info]](https://www.ccn-cert.cni.es/publico/ens/ens/1153.htm#mp.info) | Protection of information |
| All | applicable | = | = | [[mp.info.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1154.htm#mp.info.1) | Personal data |
| C | applicable | + | = | [[mp.info.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1155.htm#mp.info.2) | Qualification of information |
| C | n.a. | n.a. | applicable | [[mp.info.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1156.htm#mp.info.3) | Encryption |
| I A | applicable | + | ++ | [[mp.info.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1157.htm#mp.info.4) | Electronic signature |
| T | n.a. | n.a. | applicable | [[mp.info.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1158.htm#mp.info.5) | Time stamps |
| C | applicable | = | = | [[mp.info.6]](https://www.ccn-cert.cni.es/publico/ens/ens/1159.htm#mp.info.6) | Cleaning of documents |
| D | applicable | = | = | [[mp.info.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1160.htm#mp.info.9) | Backups. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | [[mp.s]](https://www.ccn-cert.cni.es/publico/ens/ens/1161.htm#mp.s) | Protection of services |
| All | applicable | = | = | [[mp.s.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1162.htm#mp.s.1) | Protection of electronic mail |
| All | applicable | = | + | [[mp.s.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1163.htm#mp.s.2) | Protection of web services and applications |
| D | n.a. | applicable | + | [[mp.s.8]](https://www.ccn-cert.cni.es/publico/ens/ens/1164.htm#mp.s.8) | Denial of service protection |
| D | n.a. | n.a. | applicable | [[mp.s.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1165.htm#mp.s.9) | Alternative media |

Table 41 Selection of Security Measures.

|  |
| --- |
| **Specific Controls in the management of Personal Data Breaches** |
| Contingency plans for a personal data breach. |
| Establishment of technical resources for the automatic detection of personal data breaches. |
| Incident management tools adapted to the requirements of the GDPR. |
| Protocols for the identification of potential breaches in user or data subjects complaints or communications. |
| Ability to assess the severity of the data breach. |
| Procedures for accurately describing the impact of a data breach on rights and freedoms. |
| Agile internal channels for communication of the data breach to the DPO, if appointed. |
| Agile channels of communication between the controller and the processor regarding the data breaches. |
| Procedure for deciding how to act in relation to the protection of rights and freedoms in the face of the breach. |
| Procedures for notifying the Supervisory Authority in order to comply with the requirements of Article 33. |
| Procedures for communication to data subjects in order to comply with the requirements of Article 34. |

Table 42 Specific Controls in the processing of Personal Data Breaches.

|  |  |
| --- | --- |
| **Target** | **Controls** |
| People capability | Ability to detect changes |
| Ability to communicate them |
| Ability to understand them |
| Ability to innovate |
| Ability to act in real time |
| Willingness to act proactively |
| Adequate flow of information | Agile |
| Specific |
| Minimum |
| Complete |
| From and to the right people |
| Leadership | Clear points of decision making Well-defined responsibilities. |
| Strategic adaptability | Physical, technological and organisational structures need to be able to evolve in real time towards new objectives or  ways of acting. |

Table 43 Resilience-Related Controls.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dimension** | Level | | | **SECURITY MEASURES** | |
|  | **B** | **M** | **A** |
|  |  |  |  | **org** | **Organisational framework** |
| F,E | applicable | = | = | [[org.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1078.htm#org.4) | Authorisation process |
|  |  |  |  | **op** | **Operational framework** |
|  |  |  |  | [[op.pl]](https://www.ccn-cert.cni.es/publico/ens/ens/1080.htm#op.pl) | Planning |
| F,E | applicable | + | ++ | [[op.pl.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1081.htm#op.pl.1) | Risk analysis |
| F,E | n.a. | applicable | ++ | [[op.pl.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1085.htm#op.pl.5) | Certified components |
|  |  |  |  | [[op.exp]](https://www.ccn-cert.cni.es/publico/ens/ens/1094.htm#op.exp) | Exploitation |
| F,E | n.a. | applicable | = | [[op.exp.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1097.htm#op.exp.3) | Configuration Management |
| F,E | applicable | = | = | [[op.exp.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1098.htm#op.exp.4) | Maintenance |
| F,E | n.a. | applicable | = | [[op.exp.5]](https://www.ccn-cert.cni.es/publico/ens/ens/1099.htm#op.exp.5) | Change Management |
| F,E | applicable | = | = | [[op.exp.7]](https://www.ccn-cert.cni.es/publico/ens/ens/1101.htm#op.exp.7) | Incident management |
| F,E | applicable | = | = | [[op.exp.9]](https://www.ccn-cert.cni.es/publico/ens/ens/1103.htm#op.exp.9) | Incident management log |
|  |  |  |  | [[op.ext]](https://www.ccn-cert.cni.es/publico/ens/ens/1106.htm#op.ext) | External services |
| F,E | n.a. | applicable | = | [[op.ext.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1107.htm#op.ext.1) | Contracting and service level agreements |
| F,E | n.a. | applicable | = | [[op.ext.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1108.htm#op.ext.2) | Daily management |
|  |  |  |  | [[mp.per]](https://www.ccn-cert.cni.es/publico/ens/ens/1127.htm#mp.per) | Personnel management |
| F,E | applicable | + | ++ | [[mp.per.3]](https://www.ccn-cert.cni.es/publico/ens/ens/1130.htm#mp.per.3) | Awareness-raising |
| F,E | applicable | + | ++ | [[mp.per.4]](https://www.ccn-cert.cni.es/publico/ens/ens/1131.htm#mp.per.4) | Training. |
|  |  |  |  | [[mp.sw]](https://www.ccn-cert.cni.es/publico/ens/ens/1150.htm#mp.sw) | Protection of computer applications |
| F,E | applicable | + | ++ | [[mp.sw.1]](https://www.ccn-cert.cni.es/publico/ens/ens/1151.htm#mp.sw.1) | Development |
| F,E | applicable | + | ++ | [[mp.sw.2]](https://www.ccn-cert.cni.es/publico/ens/ens/1152.htm#mp.sw.2) | Acceptance and commissioning |

Table 44 Controls relating to Failures in the Technical Safeguards for Data Protection and Errors in Applications

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk factor** | **Intrinsic risk level** | **Controls and their characteristics** | **Residual risk level.** |
| Factor 1 | Intrinsic level 1 | Control 1 | Residual level 1 |
| Control 2 |
| … |
| .. |  |  |  |
| Factor N | Intrinsic level N | Control M | Residual level N |
| Control M+1 |
| … |
|  | **Intrinsic risk level**  **of the processing operation** |  | **Residual risk level**  **of the processing operation** |

Table 45 Assessment of Residual Risk vs. Intrinsic Risk.

|  |  |
| --- | --- |
| **Elements that trigger a risk management review cycle** | |
| **Nature** | * Changes in the identity of the controller. * Changes in processing implementation. * Changes or upgrades of technological elements. * Replacing human elements for technical elements. * Substantial changes in organisational elements. * Substantial changes in processing orders. * Detection of lack of effectiveness in the measures and guarantees included in the processing. |
| **Scope** | * Change in the processing extent. * Change in the categories of data collected. * Change in the volume of data collected. * Change in the frequency of data collection. * Change of scope (temporal or spatial). |
| **Context** | * Major changes in the organisation's purposes, governance models or culture. * Change in the situations that justified the processing operations. * Incidents and breaches that have occurred in processing or similar processing operations. * Evolution of the threat model, incidents, data breaches or applicable technologies. * Changes in the volume or typology of requests in the   exercise of the rights of data subjects.   * Changes in legal frameworks or guarantees. * Changes in the regulatory implementation framework. * Corporate, political, economic or strategic changes. |
| **Purposes** | * Change or extension of the primary or   secondary purposes of processing. |

Table 46 Elements triggering a risk management review cycle.

|  |
| --- |
| **OBLIGATION TO CARRY OUT THE DPIA** |
| "Where a type of processing, in particular if it uses new technologies, is likely, by its nature, scope, context or purposes, to result in a high risk to the rights and freedoms of natural persons” 21 |
| It falls within one of the cases set out in Article 35.3 of the GDPR. |
| There is a special rule requiring an DPIA for processing. |
| Where the processing corresponds to one of the examples of obligation listed in the WP248 Guidelines. |
| When the processing meets at least two of the conditions listed in the WP248 Guidelines for conducting a DPIA. |
| Where the processing meets two or more of the criteria of the *list of the kind of*  *processing operations which are subject to the requirement for a data protection impact assessment (art 35.4)* published by the AEPD. |
| When a high risk has been assessed taking into account the cases listed in Article 28.2 of the LOPDGDD. |
| Where in any of the guidelines issued by the EDPB, the processing is identified as being required to carry out a DPIA. |
| The processing is subject to a code of conduct or a certification mechanism requiring the controller to carry out an impact assessment. |

Table 47 Obligation to carry out the DPIA

21 Article 35(1) of the GDPR and Recital 76

|  |  |  |
| --- | --- | --- |
| Judgement of suitability | It must be determined whether the processing is fit for purpose. Processing responds to certain objective deficiencies, demands, requirements, obligations or opportunities and can meet the following purposes  proposed with sufficient effectiveness. | |
| Judgement of necessity | It must be determined whether the intended purpose cannot be achieved in another less harmful or invasive way, i.e. there is no alternative processing that is equally effective  in achieving the intended purpose. | |
| Judgement of proportionality in the strict sense | The seriousness of the risk to rights and freedoms, and its intrusion into privacy, must be appropriate to the aim pursued and proportionate to the urgency and severity of the processing. The benefit that the processing, from a data protection point of view22, provides to society has to be weighed against the impact on other fundamental rights. However, even if it may partially give way, in no case can one assume the absolute denial of the right to data protection and  empty it of its essential content. |

Table 48 Judgement of Suitability, Necessity and Proportionality in the Strict Sense.

22 Recital 4 GDPR: *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."*

|  |  |
| --- | --- |
| Precise determination of the aims of the  processing. | Final, specific, measurable, achievable and bounded. |

**Judgement of suitability**

|  |  |
| --- | --- |
| Defining the threshold of processing effectiveness | Establishing, in an objective, qualitative and evidence-based manner, what is the threshold of effectiveness that should be achieved to meet the aims of the  processing. |
| Assessment of the effectiveness of the processing proposal | Assessing, in an objective, qualitative and evidence-based manner, the effectiveness of the processing as it has been planned, verifying whether it responds to the  needs and to what extent. |

**Judgement of necessity**

|  |  |
| --- | --- |
| Determination of the relevance of the purposes of processing | Assessing that the purposes of processing are of sufficient importance to be addressed by high-risk processing. |
| Verification of the  adequacy of processing operations | Verification that each of the specific processing operations is aimed at fulfilling the purposes of the processing in an objective and demonstrable manner. |
| Justification of the current processing setting | Assessing that there are no other processing, already underway or that could be considered, that address the stated purposes without incurring a high risk, even if some  modification is necessary to meet the stated purposes. |

|  |  |
| --- | --- |
| Validity clauses provided for in the processing | Regarding its nature |
| Regarding its scope |
| Regarding its context |
| Regarding its purposes |

**Judgement of proportionality in the strict sense**

|  |  |
| --- | --- |
| Identification of the degree of impact of the processing on rights and freedoms | Expressing, in detail, the limitations or intrusions to the rights and freedoms that the processing may entail for the data subject. This assessment is a prior task that has already been carried out in the determination of the risk factors and risk levels analysed previously, and its conclusions are set out at this  point in the assessment. |
| Identification and description of compensatory measures | Detailing the controls put in place in the processing design to mitigate the impact. |
| Identifying the benefits of processing | Determining the purpose and evidenced benefits and advantages of processing for individual and collective data subjects. In other words, it is also necessary to consider the  social benefit. |
| Confirmation of the existence of identity in the quality of information | It has to be assessed whether there is symmetry in the information analysed for the weighting judgement, i.e. whether the level of analysis in relation to the impact is equal to the level reached on the basis of the information provided  regarding the benefits. |
| BHB (Benefit-Harm Balance) analysis | Assessing whether the benefits to the data subjets and society, previously determined, outweigh and justify the impact on rights and freedoms  identified in point 1 of this proportionality test in the strict sense. |

Table 49 Minimum information required in the assessment of the necessity and proportionality of processing.

|  |  |
| --- | --- |
| The controller submits the prior consultation |  |
| If there is a DPO or an obligation to appoint one, he or she has advised on the data protection impact assessment and or is monitoring its implementation |  |
| If there is a DPO or an obligation to appoint one, the DPO acts as a point of contact with the Supervisory Authority |  |
| Prior consultation takes place prior to the implementation of the processing23. |  |
| The purposes of processing are objectively determined |  |
| There is a systematic description of processing operations |  |
| The assessment that the processing complies with the GDPR in terms of compliance with principles and rights has been carried out |  |
| Risk management for data subjects' rights and freedoms is documented and carried out systematically |  |
| The processing takes into account measures on the processing concept, governance and policies, data protection by design, data protection by default and security measures commensurate with managing the risk to the rights and freedoms of data subjects |  |
| The analysis of the obligation to carry out the DPIA or, as the case may be, of the need to carry out the DPIA has been carried out |  |
| The processing exceeds the necessity and proportionality analysis in relation to the purposes |  |
| All of the above actions are formally documented |  |

Table 50 Minimum requirements for the submission of a prior consultation.

23 See section "Exceptions to performing the DPIA prior to the start of processing activities"

1. Wp248: "Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals’ political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients’ medical records or a private investigator keeping offenders’ details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications [↑](#footnote-ref-1)