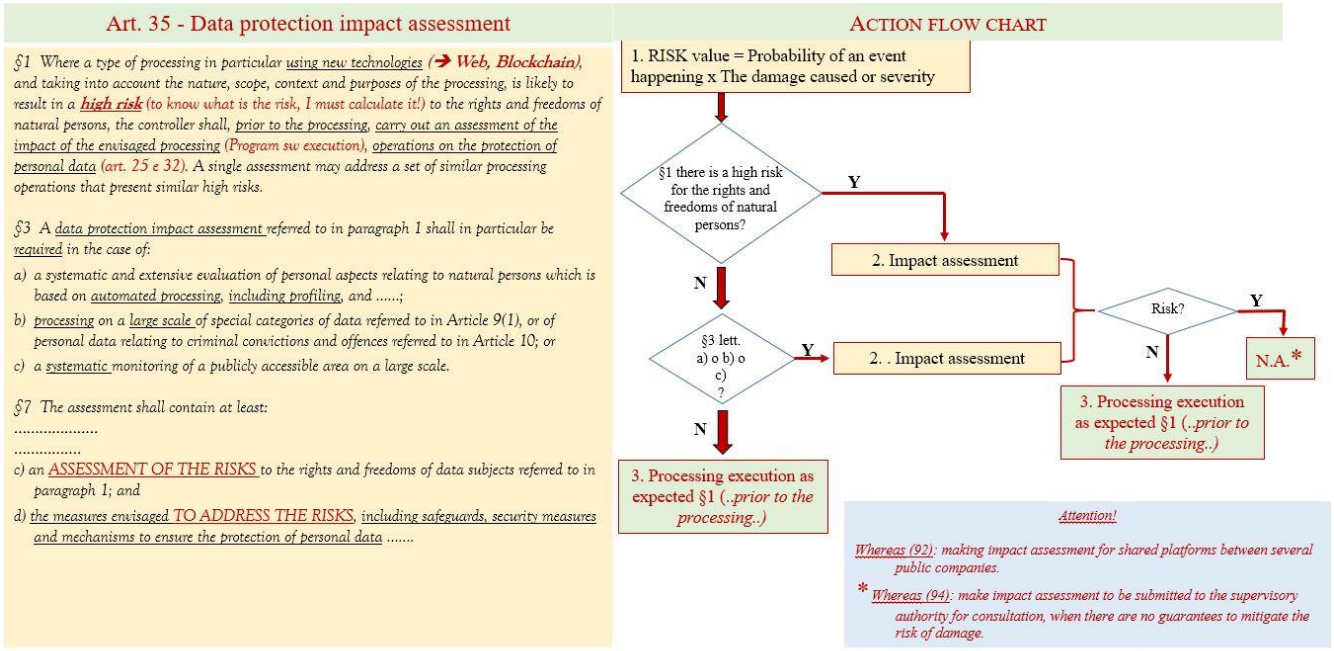
DATA PROTECTION IMPACT ASSESSMENT - RISK ASSESSMENT (ART. 35)

WHAT IS DPIA?

If there is a high risk, the Controller must ensure compliance with laws, regulations and privacy policy requirements.

That is, if on the rights and freedoms of natural persons, the damage impacts on the amount of public or on the extent of the damage, the Controller may not carry out the processing unless authorized by the supervisory authority, following the consultation.



Pedico Aldo © - Teleion S.r.l via Ferrero 31 - 10098 Rivoli (TO) - Tel. 3482244924 – email: a.pedico@teleion.it 26

NINE CRITERIA FOR THE DEFINITION OF A SET OF TREATMENTS TO CARRY OUT THE DPIA - WP248

The general data protection regulation does not require the implementation of a data protection DPIA for each treatment that may present risks to the rights and freedoms of individuals. The implementation of a data protection DPIA is mandatory only if the processing "could present a high risk for the rights and freedoms of natural persons" (art. 35, §1, illustrated by art. 35, §3, and supplemented by art. 35, §4). It is particularly important when a new data processing technology is introduced.

In cases where it is unclear whether a data protection DPIA is required or not, WP29 recommends performing it anyway, as this assessment is a useful tool that assists processing owners in complying with data protection law .

Although a DPIA on data protection may also be required in other circumstances, the art. 35, §3, provides some examples of cases in which a treatment "may present high risks":

a) *a systematic and global assessment of personal aspects relating to natural persons, based on automated processing, including profiling, and on which decisions are based that have legal effects or have a similar impact on said natural persons;*

b) *the processing, on a large scale, of special categories of personal data pursuant to art. 9, §1, or data relating to criminal convictions and crimes pursuant to art. 1013; or*

c) *systematic surveillance on a large scale of an area accessible to the public.*

In order to provide a more concrete set of treatments that require a DPIA on data protection by virtue of their inherent high risk, taking into account the particular elements referred to in art. 35, §1 and art. 35, §3, letters from a) to c), the list to be adopted at national level pursuant to art. 35, §4, and of the whereas 71, 75 and 91, and other references of the

general data protection regulation to treatments that "may present a high risk", the following nine criteria must be considered.

1. *Evaluation or assignment of a score, including profiling and forecasting, in particular in consideration of "aspects concerning professional performance, economic situation, health, preferences or personal interests, reliability or behavior, the location or movement of the interested party "(whereas 71 and 91).*
2. *Automated decision-making process that has legal effect or has a similar impact significantly: treatment that aims to allow for the adoption of decisions regarding the parties that "have legal effects" or that "have a similar impact on said natural persons" (art. 35, §3, letter a)).*
3. *Systematic monitoring: treatment used to observe, monitor or control data subjects, including data collected through networks or "systematic large-scale surveillance of a public area" (art. 35, §3, letter c)).*
4. *Sensitive data or highly personal data: this criterion includes special categories of personal data as defined in art. 9 (for example information on people's political opinions), as well as personal data relating to criminal convictions or crimes pursuant to art. 10. These personal data are considered to be sensitive (in the sense in which this term is commonly understood) because they are linked to activities of a personal or domestic nature (such as electronic communications whose confidentiality must be protected) or because they influence the exercise of a fundamental right (such as location data, the collection of which calls into question the freedom of movement) or because the violation in relation to these data clearly implies serious repercussions on the daily life of the person concerned (think for example of data that could be used for payment fraud).*
5. *Treatment of large-scale data: the general data protection regulation does not define the concept of "large-scale", however it does provide a guideline with regard to whereas 91. In any case, WP29 recommends taking into account, in particular , of the factors listed below in order to establish whether a treatment is carried out on a large scale:*
   a) *the number of subjects involved in the treatment, in absolute terms or expressed as a percentage of the reference population;*
   b) *the volume of data and / or the different types of data being processed;*
   c) *the duration, or persistence, of the processing activity;*
   d) *the geographical scope of the processing activity;*
6. *Creation of correspondences or combination of data sets;*
7. *Data relating to vulnerable persons (whereas 75);*
8. *Innovative use or application of new technological or organizational solutions: for example, some applications of "Internet of things" could have a significant impact on the daily life and private life of people and, consequently, require the realization of a DPIA on the data protection.*
9. *When the treatment in itself "prevents the interested parties from exercising a right or from making use of a service or a contract" (art. 22 and whereas 91).*

WHEN DPIA IS NOT REQUIRED – WP248

WP29 believes that a DPIA on data protection is not required in the following cases:

a) when the processing is not such as to "present a high risk for the rights and freedoms of natural persons" (art. 35, §1);

b) when the nature, scope, context and purpose of the processing are very similar to a treatment for which a data protection impact assessment has been carried out.

c) when the types of processing were verified by a supervisory authority before May 2018 under specific conditions that have not changed (see III.C);

d) if a treatment, carried out in accordance with the art. 6, §1, letters c) or e), find a legal basis in Union law or in the law of the Member State, this right governs specific treatment or an impact assessment has already been carried out on data protection in the context of adoption of this legal basis (art. 35, §10), unless a Member State has declared that it is necessary to carry out this assessment before proceeding to the processing activities;

e) if the processing is included in the optional list (established by the supervisory authority) of the types of processing for which no impact assessment is required on data protection (art. 35, §5);

f) a data protection DPIA is not required for the treatments that have been verified by a supervisory authority or by the DPO, according to the art. 20 of Directive 95/46/EC and which are carried out in such a way as to ensure that no change has been recorded with respect to the previous verification.

MINIMUM CHARACTERISTICS OF A DPIA – WP248

The general data protection regulation defines the minimum characteristics of an impact assessment on data protection (art. 35, §7, and whereas 84 and 90):

1. *a description of the treatments envisaged and the purposes of the processing;*
2. *an assessment of the necessity and proportionality of the treatments;*
3. *an assessment of the risks to the rights and freedoms of the data subjects;*
4. *the measures envisaged for:*
   - ✓ *face risks;*
   - ✓ *demonstrate compliance with this regulation.*

In assessing the impact of a treatment, it is necessary to take into account (art. 35, §8) compliance with a code of conduct (art. 40). This can be useful to show that adequate measures have been chosen or implemented, provided that the code of conduct is appropriate to the treatment operation concerned. Certifications, seals and trademarks must also be taken into consideration in order to demonstrate compliance with the general data protection regulation of data processing performed by data controllers and data processors (art. 42), as well as with respect to the binding rules of company.

All the relevant requirements set out in the general data protection regulation provide a broad and general framework for the design and implementation of a data protection DPIA.

The whereas 90 of the general data protection regulation outlines a series of elements of the DPIA on data protection that overlaps with well-defined elements of risk management.

In terms of risk management, an impact assessment on data protection aims to "manage risks" for the rights and freedoms of individuals, using the following processes:

1. establishing the context: "*taking into account the nature, the field of application, the context and the purposes of the treatment and the sources of risk*";
2. evaluating the risks: "*assessing the particular probability and seriousness of the risk*";
3. dealing with the risks: "*mitigating this risk*" and "*ensuring the protection of personal data*", and "*demonstrating compliance with this regulation*".

PUBLICATION DPIA – WP248

The publication of a DPIA is not a legal requirement enshrined in the General Data Protection Regulation, it is a decision of the Controller to proceed accordingly. However, controllers should consider publishing at least some parts, such as a summary or the conclusion of their DPIA.

CRITERIA FOR AN IMPACT ASSESSMENT ON THE ACCEPTABLE DATA PROTECTION – WP248

The WP29 proposes the following criteria that the data controllers can use to establish whether an impact assessment is required on data protection or not or if a methodology for carrying out such an assessment is sufficiently complete to ensure compliance with the general regulation on data protection:

a) a systematic description of the treatment is provided (art. 35, §7, lett. a)):

1. the nature, scope of application, context and purpose of the processing are taken into consideration (whereas 90);
2. personal data, recipients and period of storage of personal data are recorded;
3. a functional description of the treatment is provided;
4. the resources on which personal data are based are identified (hardware, software, networks, people, paper channels or paper transmission);
5. the compliance with the approved codes of conduct is taken into consideration (art. 35, §8);

b) necessity and proportionality are assessed (art. 35, §7, lett. b)):

1. the measures envisaged to guarantee compliance with the regulation have been determined (art. 35, §7, lett. D) and whereas 90):
   - ❖ measures that contribute to proportionality and the need for treatment based on:
     - Ψ determined, explicit and legitimate purposes (art. 5, §1, lett. B));
     - Ψ lawfulness of processing (art. 6);
     - Ψ adequate, pertinent and limited personal data as required (art. 5, §1, lett. c));
     - Ψ limitation of conservation (art. 5, §1, lett. E));

- measures that contribute to the rights of the interested parties:
  - information provided to the interested party (art. 12, 13 and 14);
  - right of access and portability of data (art. 15 and 20);
  - right of rectification and cancellation (art. 16, 17 and 19);
  - right to object and limitation of treatment (art. 18, 19 and 21);
  - relations with data processors (art. 28);
  - guarantees concerning international treatments (Chapter V);
  - preventive consultation (art. 36).

c) the risks for the rights and freedoms of the interested parties are managed (art. 35, § 7 letter c):

1. the origin, nature, particularity and gravity of the risks (see whereas 84) or, more particularly, for each risk (illegitimate access, undesired modification and disappearance of the data) are determined by the perspective of the interested parties:
   - risk sources are considered (whereas 90);
   - potential impacts are identified for the rights and freedoms of data subjects in the event of events that include illegitimate access, unwanted modification and disappearance of data;
   - threats are identified which could lead to illegitimate access, unwanted modification and disappearance of data;
   - probability and gravity are estimated (whereas 90);
2. the measures envisaged to manage these risks are established (art. 35, §7, lett. D) and whereas 90);

d) interested parties are involved:

1. the data protection officer is consulted (art. 35, §2);
2. the opinions of the interested parties or their representatives are collected, where appropriate (art. 35, §9).

ADVANTAGES FOR CARRYING OUT DPIA

This international standard provides a guide that can be adapted to a wide range of situations in which PII is processed. However, in general, a DPIA can be performed for the purpose of:

a) identify impacts, risks and responsibilities on privacy;
b) provide input to design for the protection of privacy (art. 25);
c) review the privacy risks of a new information system and assess its impact and probability;
d) provide the basis for the provision of privacy information for the main PII on any mitigation action;
e) keep subsequent updates with additional features;
f) share and mitigate risks with interested parties; providing compliance information.

NOTE. A DPIA is sometimes referred to by other terms: "Privacy Review"; "DPIA".

The costs of modifying a project at the planning stage is usually a fraction of those incurred later.

If the impact is unacceptable, the project can be canceled completely.

However, a DPIA helps to identify problems early and reduce management time costs, legal and potential media or public interest costs, taking into consideration problems in advance.

It can also help an organization avoid costly mistakes and embarrassing privacy.

Although a DPIA should be more than just a compliance check, it still helps to demonstrate an organization's compliance with relevant privacy and data protection requirements in the event of a subsequent complaint investigation, privacy check or compliance. In the event of a privacy risk or a breach occurring, the DPIA report may provide evidence that the organization has acted appropriately in an attempt to prevent occurrence. This can help reduce or even eliminate any liability, negative publicity and loss of reputation.

DPIA increases an informed decision-making process and exposes gaps in internal communication or hidden hypotheses on privacy issues regarding the project.

DPIA allows the organization to know in advance the pitfalls to the privacy of a process, a computer system or a program, rather than having its auditors or competitors make them notice it.

DPIA can help:

1. an organization to gain public trust and confidence that privacy was built in the design of a process, an IT system or a program;
2. to anticipate and respond to public concerns about privacy.

OBJECTIVES OF DPIA SIGNALS

The objective of DPIA reporting is to communicate the results of the assessment to the interested parties and to meet their expectations.

The following examples are typical of a stakeholder expectation:

a) Main PII - DPIA is a tool to allow PII subjects to be sure that their privacy is protected.

b) Management - different points of view apply with:

1. the DPIA as a tool to manage privacy risks, create awareness and establish responsibilities; visibility beyond PII processing within the organization, and possible risks, impacts thereof;
2. carrying out the DPIA in the early stages of the project guarantees that the privacy requirements are included in the functional requirements and not, are achievable, are vital and are tracked through change and risk management; the effort to classify and manage PII projects should be financed as a separate investment line and quantified in a project budget;
3. the DPIA is a tool to understand the risks for privacy to / project / unit level the function; risk consolidation; Entry to the design and application mechanisms on Privacy; inputs for the re-Engineering privacy processes.

c) Regulator - DPIA is a tool that helps provide evidence for compliance with applicable legal requirements. It is able to provide proof of due acts adopted by the organization in the event of violation, non-compliance, denunciation, etc.

d) Customer - DPIA is a means to assess how the PII processor or PII owner is managing PII and provides evidence that follows contractual obligations.

The reporting of DPIA should perform two basic functions.

a) Inventory: keeps the specific subjects informed of the affected entities, the environment concerned and the risks on the life cycle of the affected entities.

b) Action items: it is a mechanism for monitoring the actions / activities that improve and / or resolve the identified risks. The sensitivity for the distribution and disclosure of reporting information must be clearly assessed and classified (private, confidential, public, etc.).

RESPONSIBILITY TO CONDUCT DPIA

In general, the responsibility for ensuring that a DPIA has been undertaken should, firstly, if there is one, the PII protection officer, otherwise with the person responsible for the new technology, service or development project. another initiative that may impact on privacy.

When the DPIA is performed directly by the organization, end-user associations or government agencies may request to have the adequacy of the DPIA verified by an independent auditor.

The organization must ensure that there is responsibility and authority for risk management, including the implementation and maintenance of the risk management process and to ensure the adequacy and effectiveness of the controls.

This can be facilitated by:

a) specify who is responsible for the development, implementation and maintenance of the risk management framework; is

b) specify the owners of the risk for the implementation of the risk treatment, maintaining the privacy controls and the communication of the relevant information the risk.

IMPACT ASSESSMENT METHODOLOGY

The scope of a DPIA, the specific details of what it covers and how it is carried out all need to be adapted to the size of the organization, the territorial competence and the specific program, the information system or a process that is the subject of the DPIA.

The organization conducting a DPIA process may wish to directly adapt the process guide followed for its specific DPIA scale and purpose or as a possible alternative to select an appropriate risk-based management system, such as ISO / IEC 27001, and integrate into appropriate way elements of the guide below, including the use of the DPIA report for the treatment of privacy risks identifying.

In this international standard, the term “conducting a DPIA” is used to cover both an initial DPIA in which the steps and actions necessary to satisfy the particular DPIA requirement are selected; and an update to an existing DPIA where only the steps and actions necessary for the update are performed.

Annex C provides further guidance on understanding the terms used in this international standard.

NOTE. To support SMEs in the DPIA process, trade associations or small and medium-sized enterprises should be encouraged to draft codes of conduct by providing valuable guidelines, and SMEs should be encouraged to participate in these activities. Reasonable codes of conduct should respect the values set forth in this international standard and could get approved by data protection authorities.

The methodological steps for achieving the objective are listed below.

a) Establishment of the DPIA group and provide them with management.
b) Preparation of a DPIA plan and determination of resources to conduct the assessment.
c) Describe what is being evaluated.
d) Identification of stakeholders.
e) Establish a consultation plan.
f) Consult with stakeholders.
g) Identify the PII information flow.
h) Analyze the implications of the cases in use.
i) Determine and safeguard the privacy requirements.
j) Identification of threats and risk calculation.
k) Generic threats.
l) Threats deriving from the processing of personal data in Healthcare.
m) Calculation of damage or severity and probability levels.
n) Evaluation of the priority of the risks.
o) Classification risk.
p) Choose risk treatment actions.
q) Determine controls.
r) Create risk treatment plans.
s) DPIA.
t) Resolution.

The resolution of the DPIA must be based on the results of the risk management process that has been carried out, as well as on the residual risks and the decision to accept the risks or not to accept them.

An effective application/intelligent system will be considered satisfactory by the system manager once the DPIA process has been completed with relevant risks identified and appropriately treated to ensure the absence of residual unacceptable risks for people, and in order to meet the requirements of conformity, with appropriate internal revisions and approvals.

The following solutions can be envisaged at the end of the DPIA process:

1. An intelligent network system or application already in production:
   - ✓ DPIA positive: *the DPIA reports must be registered and kept by the organization's DPO and kept at the disposal of the data protection authority*;
   - ✓ DPIA negative: *a further examination will be necessary with a specific corrective action plan to be developed including a proposal for more efficient or new controls, and a new DPIA to be completed in order to determine whether the application has reached an approvable state*.
2. An intelligent network system or application still in the planning stage:
   - ✓ DPIA positive: *the risks have been assessed and the controls regarding these risks correctly defined and developed. Residual risks have been reported and no further controls have been identified and / or some risks have been accepted. The DPIA report should include future dates for system control when it is in production;*
   - ✓ DPIA negative: *in addition to providing further controls to obtain a new and satisfactory level of residual risks, the report should also recommend, whenever possible, the new project actions for the application following the Privacy by Design principle.*

It is important to note that the final solution should be a management decision based on the results of the assessments made, reflecting the social interest related to the development of the intelligent network.

DPIA FOLLOW UP

This process concludes the methodological process carried out within the group of processes for impact assessment.

Below is a list of the activities that make up the Follow Up of the DPIA.

A. *Report preparation*
B. *Publication*
C. *Implementation of risk treatment plans*
D. *Review and / or audit of the DPIA*
E. *Address process changes*
F. *Documentation for the DPIA*

This point gives indications on the content of the DPIA report.

The contents of the DPIA report will strongly depend on the type and sensitivity of PII being processes, its nature and the scope and objectiv.es of the DPIA conducted. Thus this guide should be interpreted in the context of the specific project.

Some of the details of the DPIA report may be confidential. They can solve business problems that should not be made public. They can address treatment options that may reveal sufficient details about residual risks to increase the risk of system compromise.

The organization should determine the appropriate audience and contents of the DPIA report and its degree of confidentiality. A trust relationship to an independent auditor or data protection authority may contain more information than is provided to interested parties or the public.

The organization should consider addressing the following issues and consider the guidance provided below.

1. The structure of the document.
2. The scope of the evaluation; the privacy requirements; risk assessment.
3. The risk treatment plan.
4. The conclusion and the decisions taken on the basis of the DPIA result.
5. A public DPIA summary suitable to be used to inform the main PII about the level of risk associated with the program, information system, and the implementation process in which their PII will be involved.

STRUCTURE OF THE DOCUMENT

The DPIA report should be adapted to specific circumstances.

Normally indicated:

a) *on its cover page:*
   1. the name of the process;
   2. the computer system or a program;
   3. the name and address of the PII manager and the organization that carries out the DPIA;
   4. the contact person with the contact details;
   5. the version number for checking documents;
   6. the date of the DPIA report; is
   7. also appoint those who can address any questions if they are different from the person who conducted the DPIA;
   8. if the DPIA report is long, it should include a summary indicating the main conclusions and recommendations of the DPIA and that the interested parties have been consulted, a brief description of the program, the information system, process or other initiative, which is been the subject of the DPIA;
   9. the reason why the DPIA was undertaken.

b) *Introduction*

   The introduction should indicate the reason why a DPIA was conducted, when it was conducted, who was involved in conducting the DPIA and the DPIA terms of reference. It should provide some information about the process, computer system or evaluation program. The guidelines used in the DPIA should be introduced (for example, the decision to involve the interested parties). The introduction should provide all the contextual information about the organization and its environment that may be needed in order to understand the motivation of the DPIA. The introduction could also refer to the organization's privacy policy or code of conduct, as well as the organization's obligations to its stakeholders (shareholders and, where applicable), as well as its compliance with relevant legislation.

c) *Information on system requirements*
d) *Information on the system architecture*

e) *Operational plans and procedures*

f) *Risk criteria*

g) *Resources and people involved*

h) *Consultation of interested parties*

i) *Privacy Requirements*

j) *Risk treatment plan*

k) *Conclusions and Decisions*

PUBLICATION

In order to provide users with information on privacy risks, whether they are external or dependent PII principles, to support the consent, a public summary of the DPIA may need to be prepared by the main DPIA report.

If necessary, the summary should remove commercially sensitive information that could be present in the full DPIA report and leave only the key aspects relevant to the main PII.

The public DPIA summary report must contain:

a) the advantages of the program, the information system or process;

b) the types of PII to be processed and collected;

c) the legal jurisdictions in which the PII treatment is carried out;

d) a summary of the compliance analyzes;

e) a list of possible measures to comply with the privacy requirements or for the treatment of privacy risks that the intentions of the organization to adopt or have adopted;

f) the measures that the main PII is recommended to take;

g) the organization responsible for the DPIA and the program, the information or process system;

h) the contact details of the responsible owner; is

i) the details of each user detected by a help desk or by a support structure for the users implemented for the program, the information system or process.

When the summary of DPIA's public addresses the main PII as members of the general public, they should represent all of the above information and all further information in a transparent, clear and understandable way.