# DISSERTATION EXAM

## AN APPROACH TO DECOMPOSE THE DATA PROTECTION IMPACT ASSESSMENT

STUDENT: PETROS GIALLELIS MTE1610

SUPERVISOR PROFESSOR: KONSTANTINOS LABRINOUDAKIS

## Contents



## ABSTRACT

This paper undertakes to decompose the notion of "Data Protection Impact Assessment" pursuant to the definition and the requirements set forth in Article 35 of Regulation (EU)

2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR" or the "Regulation"). The paper defines the exact circumstances under which the conduct of a Privacy Impact Assessment is mandatory and highlights the key points for a proper implementation from a procedural perspective.

Throughout all the aforementioned steps, additional deliberation will be provided in order to distill the terms and conditions mentioned in the Regulation, Article 29 Data Protection Working Party (hereinafter "WP29") and European Data Protection Board (hereinafter "EDPB" or the "Board") guidelines and opinions.

In order to achieve an efficient comprehension of the current document a good knowledge on the fundamental notions of privacy and security is required.

## CHAPTER 1. DECOMPOSING THE DEFINITION OF DATA PROTECTION IMPACT ASSESSMENT

According to Article 35 of the GDPR, a DPIA is an assessment of the impact of any processing activity conducted by a Data Controller to the rights and freedoms of natural persons derived by the implementation of threats which emerge by the envisaged processing operations.

### A. Risk-based approach and high risk

The definition imposes in particular the need of conducting a DPIA when "high risk" condition is met. Although the notion of "threat" is not directly mentioned in GDPR, the term "high risk" verifies that the approach of the Regulation on DPIA tends to simulate and adopt the traditional risk management methodology. Strongly indicative of the aforementioned approach are the contents of recital 84 in which the Regulation states that the controller is responsible to carry out a DPIA "to evaluate, in particular, the origin, nature, particularity and severity of that high risk " , as also the ones or recital 90 which actually describe the "context", "risk assessment" and "risk treatment" notions in terms of personal data protection .

### B. New technologies and their security perspective

The presence of the phrase "in particular using new technologies" in the definition, should be interpreted as a complementary statement to the "high risk" condition. The fact that

there is a special mention to the usage of new technologies, tends to underline the increased probability to meet "high risk" condition for rights and freedoms of the data subjects once a new set of technologies is involved in the processing operation. By default the usage of new technologies gives birth to new threats and zero day attacks in terms of security, which might lead to personal data breaches. In any case the usage of new technologies should not be considered as a solid and standalone circumstance of setting the conduction of DPIA mandatory.

### C. Map the processing the Data Protection principles

In the phase of assessing whether a DPIA is required prior to a particular processing operation, the nature, the scope, the context and the purposes should be taken in consideration. On an attempt to interpret these factors, it is indirectly projected that the definition prompts Data Controllers to map the whole processing operation, which is about to be undertaken with the articles of the Regulation its requirements and its derogations and the data protection principles.

### D. Rights and Freedoms of the data subjects. Is it about Articles 15-22 of GDPR?

The usage of the term "rights and freedoms of the data subjects" constitute a shortcut to the "**Charter of fundamental rights of the European Union".** To this point it is worth to mention that a processing operation might emerge threats not only regarding the freedom to the "Protection of personal data" of Article 8, but also others such as the right of integrity, as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

## CHAPTER 2. WHEN IS A DATA PROTECTION IMPACT ASSESSMENT REQUIRED?

Paragraph 3 of Article 35 GDPR sets forth three instances under which a DPIA is mandatory. It is of great importance to pay attention to the term "in particular". The term leads to an understating that paragraph 3 actually describes three examples in abstract

terms, which if at least one of them is met, a Data Controller shall undertake to conduct a DPIA. However, the term "**in particular**" indicates that the list should be considered as **non-exhaustive** by Data Controllers.

The WP29 "**Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" adopted on the 4th of April of 2017 and revised on the 4th of October of 2017**, provide a much more detailed list of categories/conditions which might set a DPIA mandatory, accompanied by a metric/framework which can assist Data Controllers in their assessment of whether a DPIA is required as well as its scope.

In an attempt to present and simplify the aforementioned framework designed by WP29, the procedure of identifying the "high risk", is to identify at least two matching conditions of the list below:

### Evaluation or scoring

This condition depicts any processing operation, which aims to extract information on data subject's performance at work, economic situation, health status, interests and reliability.

In other words WP29 describes the notion of "profiling" as defined in Article 4 of the Regulation.

### Automated-decision making with legal or similar significant effect

This condition includes any potential data processing which leads to decision making about data subjects with significant legal effect.

Automated decision making, must be examined in conjunction with Article 22 of the Regulation which sets out the right of a natural person not to be subject of decisions based solely on automated processing and the Article 35(3)(a).

### Systematic monitoring

This condition, is set out in Article 35(3)(c) and applies to processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area"

### Sensitive data or data of a highly personal nature

This condition refers to any data processing conducted on data which fall under Article 9 and Article 10. On an attempt to give an abstract description of these data, we would say that this condition includes all data linked to household and private activities or they

impact the exercise of a fundamental or their violation clearly involves serious impacts in the data subject's daily life

It is worth to mention that while deliberating on this condition, the wp29 defines includes all the above under the term "sensitive data", while on the meantime underlines that is not an official one ("this term is commonly understood").

### Data processed on a large scale

This condition has an abstract nature both in Regulation, as also in wp29 guidelines.

The Regulation just mentions in Article 35(3)(c) the term "large scale", without any supplementary clarifications, while the WP29 attempts to decompose the term by providing four(4) factors which should be estimated when assessing if "large scale" processing exists :

- the number of data subjects concerned, either as a specific number or as a proportion of the relevant population
- the volume of data and/or the range of different data items being processed
- the duration, or permanence, of the data processing activity
- the geographical extent of the processing activity

### Matching or combining datasets

This condition applies to cases where two or more data processing operations are performed for different purposes and/or by different Data Controllers in a way that would exceed the reasonable expectations of the data subject. This condition must also include the case of two different datasets, where in each dataset different data for the same data subject exist.

The significance of this condition is indirectly underlined in the WP29 "**Opinion 05/2014 on Anonymisation Techniques**" , where the authors point out that in order to implement a robust anonymisation procedure, it must be taken in consideration that the dataset remains anoynimised even if it is combined with another dataset or data available in public.

### Data concerning vulnerable data subjects

This condition intends to bring in the foreground data processing related to data processing where increased power imbalance between the data subjects and the data controller exists.

Such cases might include data processing related to children which are unable to easily consent to, or oppose, the processing of their data, or exercise their rights (recital 38 of

the Regulation), employees where the role of data controller is fulfilled by the employer or more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients).

### Innovative use or applying new technological or organizational solutions

As introduced in Article 35(1) and recitals 89 and 91 of the Regulation, it is considered to be a constant that any use of a new technology might include novel forms of data collection and usage, triggering potentially high risk to individuals' rights and freedoms.

### When the processing in itself "prevents data subjects from exercising a right or using a service or a contract

This condition includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. It must always stay important during the DPIA the set of derogations which accompany this condition (Article 22 of the Regulation)

As supplementary material and with the tension to create a statutory framework of the cases when DPIA is required, the statements below must be taken in consideration:

- The more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt. However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.
- The Regulation encourages the data protection authorities to establish lists with categories of processing operations which fall into the requirement and with ones that do not fall. It is of great importance to outline that these lists should not be considered as absolute ones, as far it is not feasible to include proactively any processing operation and the time frame in which these lists will be published is not certain.

While describing the circumstances under which Dpia is mandatory, it is worth describing **UK ICO's** framework for evaluating whether a data processing operation, requires the conduction of a privacy impact assessment.

ICO provided to Data Controllers 8 questions, to which they have to answer with "yes" or "no" , without derogations or exceptions. The questions are the ones below :

1) **Will the project involve the collection of new information about individuals?**

2) Will the project compel individuals to provide information about themselves?

3) Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?

4) Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

5) Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

6) Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

7) Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

8) Will the project require you to contact individuals in ways that they may find intrusive?

If data controllers answer with a "yes" to at least one of these questions, then a strong indication that a dpia is required emerges.

## CHAPTER 3.CHARACTERISTICS AND MINIMUM REQUIREMENTS FOR CONDUCTING A COMPLIANT DPIA

The Regulation does not provide nor does it propose a structured procedure on how to implement properly a DPIA. Paragraph 7 of Article 35 deploys a list of minimum

requirements which must be met in any DPIA implementation in order to be considered as a valid one, while on the meantime offers flexibility to Data Controllers on the procedural part of the implementation.

On the section below, an attempt to decompose and analyze the aforementioned requirements will take place:

## A. The description of the envisaged processing operations and processing purposes

The first criteria which must be met in a DPIA, is "a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller ":

This first condition actually prompts Data Controllers to describe their processing operations, not in terms of privacy and security exclusively, but also from an operational perspective. The intention of this requirement is to assist controllers recognize all the aspects of their activities, in order to be able in later steps to reach the optimum data privacy impact assessment. Apart from the description of the processing activities in itself, the Regulation prompts the conductors of the DPIA, to accompany the description with the purpose of processing. This approach, tends to assist conductors ensure that there won't be an infringement of the principle of "purpose limitation" as posed in Article 5 of GDPR. The special mention to the "legitimate interest pursued by the controller" is extremely important, as it can be inferred that the Regulation underlines the severity and the peculiar circumstances when Data Controllers assess that their legitimate interest is not overriding the fundamental rights and freedoms of the data subjects. In fact the mention of the phrase "legitimate interest pursued by the controller", is probably triggered due to the fact that the legitimate interest might be claimed to be the legal basis for the data processing as per Article 6.

Under the systematic description of the processing, the Data Controller details the nature, the scope, the context and the purposes of the envisaged data processing.

The systematic description of the processing also requires the identification of the assets on which personal data reply. The term "assets", refers to the medium where personal data is located, stored or transmitted and includes hardware, software, networks, people, paper or paper transmission channels. While this step of the assessment entails a technical appreciation of the processing scheme, it is of particular importance in order to identify potential risks of data breach and address them preventively.

It is worth to mention, that although the Regulation does not require from data processors to conduct a DPIA directly, Article 28 GDPR requires processors to process personal data on behalf of Controllers following a written agreement setting out the same elements as the ones set forth in a DPIA. Thus, data processors are required to abide by the requirements of the Controller's DPIA without conducting one themselves. This is due to the fact that Data Controllers are ultimately the ones to hold information on the nature and purpose of the processing, the type of personal data and categories of data subjects that their activities entail.

## B. Necessity and proportionality assessment

The second criteria is much more direct regarding its outcome and its intention, as the terms "an assessment of the necessity and proportionality of the processing operations in relation to the purposes", prompts Data Controllers to conduct their processing activities in compliance with:

- the principle of necessity, which constitutes a fundamental principal when assessing the restriction of fundamental rights,
- the principle of proportionality, which is a general principle of EU law with the intention to restrict authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim and particularly in the context of fundamental rights, such as the right to the protection of personal data. The principal of proportionality is key for any limitation on such rights.
- the principle of data minimisation, which mandates Data Controllers to limit the processing of personal that is "necessary in relation to the purposes for which they are processed" (Article 5(1)(c)) , and
- the principle of storage limitation, which mandates that data controllers will not retain personal data of the data subjects, for a period greater than the one needed to fulfill the processing. (Article 5(1)(e))
- The lawfulness of processing. (Article 5(1)(b))

- According to wp29, during this phase the data controller must verify that is able to fulfill the data subjects' requests, if they potentially wish to exercise their rights, as described in Articles 12-21.

## C. Risk assessment and measures addressing potential infringements of data subjects' rights

The third criteria requires the Data Controller to investigate whether any aspect of the intended processing operations might restrict or infringe any of the rights and freedoms of the data subjects.

At this stage, the DPIA includes an assessment of the "origin, nature, particularity and severity of the risks" from the perspective of the data subjects. In particular, the DPIA attempts to establish the risks sources, the potential impacts to the rights and freedoms of data subjects in cases of data breaches (i.e. illegitimate access, undesired modification and disappearance of data), threats that could lead to data breaches and an estimated likelihood and severity. Finally, the DPIA is required to proactively set out measures taken in terms of security, safeguards and the established mechanisms to ensure the protection of the personal data to treat the determined risks. (Article 35(7)(c) and (d) GDPR).

According to (Article 35(7)(c) and (d) ) the DPIA, is implemented in an identical way, with a traditional risk assessment procedure, where the risk is defined :

*Risk = probability of a threat derived from the particular data processing X the impact on the rights and freedoms of the data subjects.*

For each risk identified in risk identification process, the Data Controller must define any mitigation actions and measures taken, in order to eliminate either the probability to occur or to eliminate the impact if this threat occurs.

If, following the above mentioned risk assessment process, the Data Controller identifies residual high risks (i.e. risks that cannot be fully mitigated by intra-organizational measures and procedures and/ or that cannot be addressed by additional measures), the GDPR imposes prior consultation with the supervisory authority (Article 36(1) and (2) GDPR) which will in turn undertake to provide advice within a strict time-frame (8 weeks).

### D. Data subject and DPO consultations

An element of great importance, during the conduction of DPIA, is the interaction with the data subjects or their representatives on the intended processing. (Article 35(7)(9))

The Data Controller shall seek the view of data subjects, in order to :

- ensure that the data controller has a lawful basis for processing any personal data
- Assess whether the mitigation measures taken and the residual risks are acceptable, prior proceeding with the data processing.

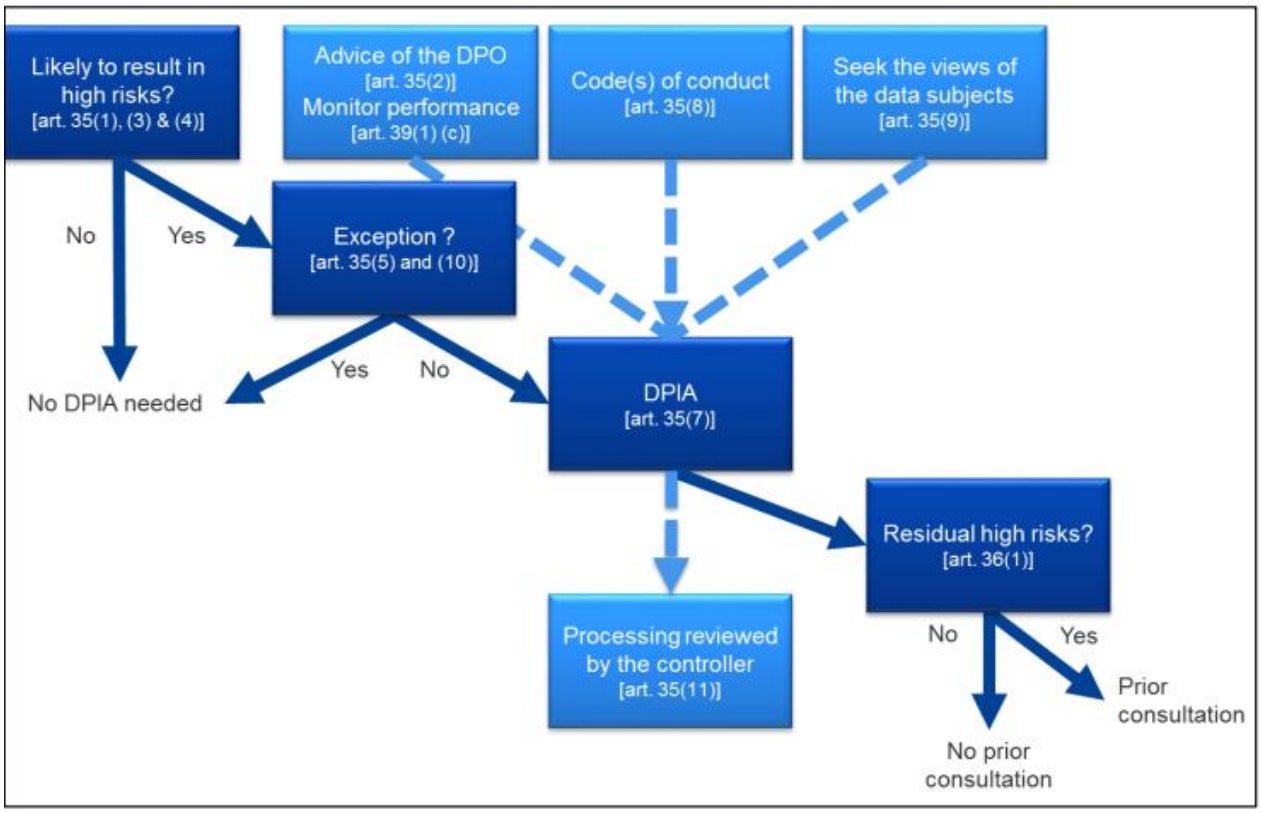
Data Controllers should involve their data protection officers (DPO), if exist, during the conduction of DPIA and its reviewing process. (Articles 37 and 39)

## CHAPTER 4.WHEN TO CARRY OUT A DPIA?

The answer to the question when DPIA should be conducted, is always prior the processing, as it is explicitly mentioned in Article 35(1) and being consistent with the principles of privacy by design and privacy by default(Article 25, recital 78)

The figure below, depicts a comprehensive summary of the logical steps each organization (data controller), should follow in chronological order, in order to:

- Assess whether DPIA is needed
- DPIA conduction and all the entities involved.
- Assess whether data protection authority consulting is needed.



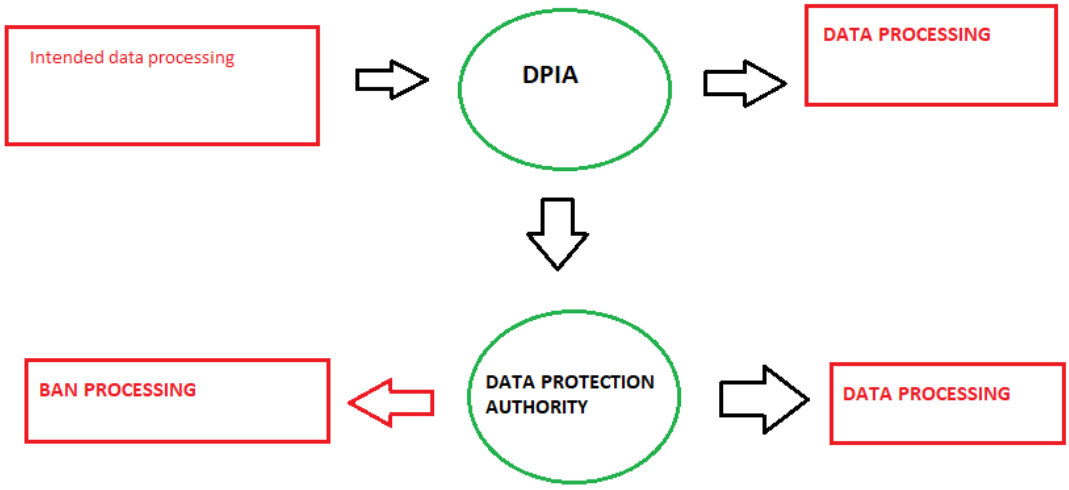

A more accurate approach is that any **potential data processing activity always follows a DPIA**, because its conduction might result the suspension of the processing activity . If the measures taken to address the risks to the rights and freedoms of data subjects, are not enough to mitigate the severity of the impact and “high risk” persists, the data controller shall seek for the consulting of the data protection authority. (Article 36(1)) . The data protection authority will receive by the data controller a set of information(Article 36(2)), including :

- he respective responsibilities of the controller, joint controllers and processors involved in the processing
- the purposes and means of the intended processing
- the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation

- the contact details of the data protection officer
- the data protection impact assessment
- several further information according to the complexity of the intended processing,

and will assess whether the data processing could infringe the regulation.

During this phase data protection authority may use any of its powers referred to Article 58, and can even impose a temporary or definitive limitation including a ban on processing. (Article 58(2)(f)).




The regulation also introduces a recursive and continuous character in DPIA according to Article 35(11). Data Controllers are prompted to assess whether deviations emerged on the risks related to the processing. The usage of a new technology, processing on a bigger

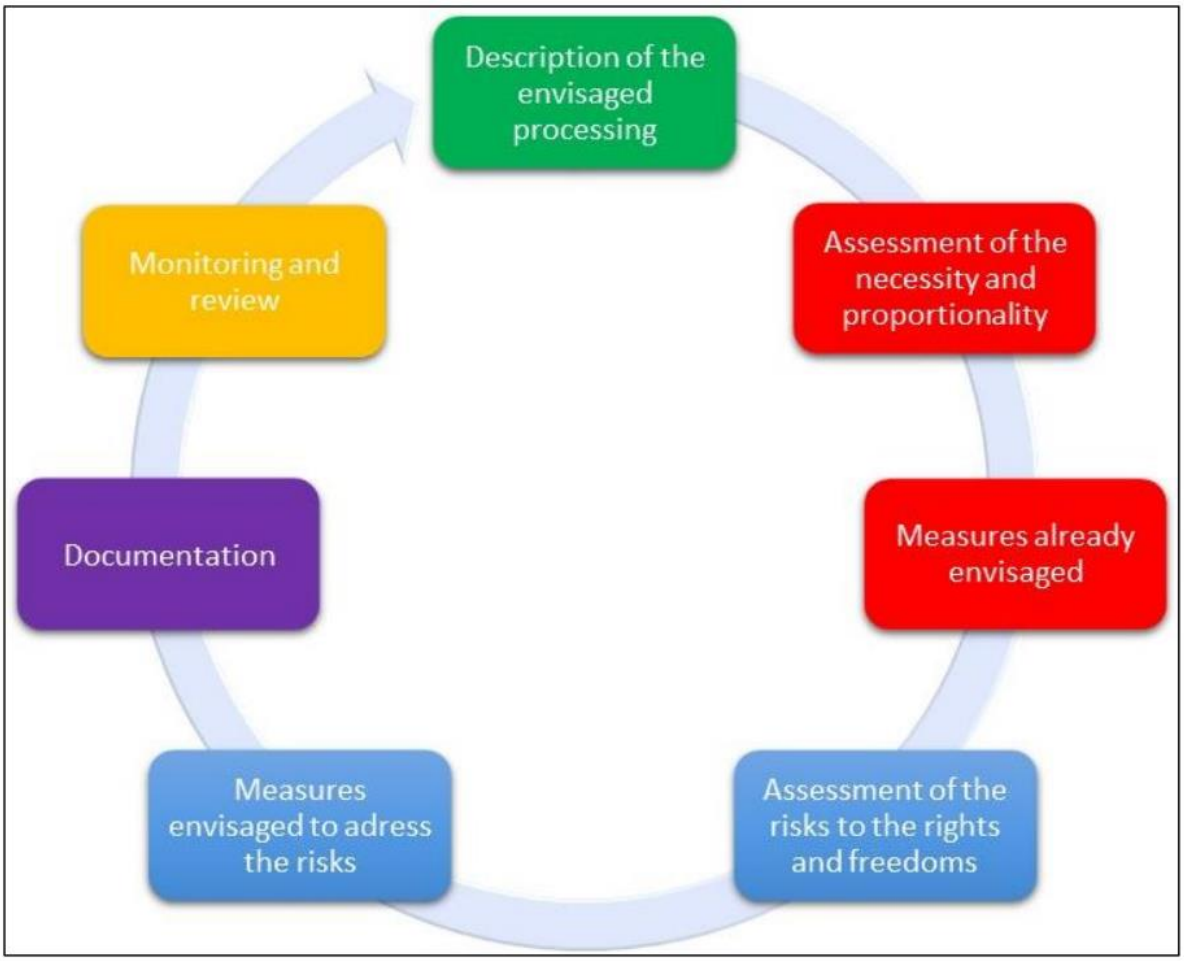
extent or a new branch of the data processing might alter the population or the severity levels of the existing risks.

It seems mandatory for data controllers to review and assess if processing is performed in accordance with the data protection impact assessment and whether new technical or organizational measures should be taken in order to ensure compliance.

The aforementioned, indicates that **DPIA is not a "once off" procedure, but an ongoing procedure alongside with the data processing** . The process should start when a project is in the early planning stage, when there is an opportunity to influence the project's design or outcome.

## CHAPTER 5. IS THERE A STRICT METHODOLOGY TO INHERIT?

On an attempt to drill down the dpia implementation, and particularly the article 35 (7), similarities are met with the plan-do-check-act (PDCA) model. The figure below, by wp29 guidelines, depicts perfectly the risk based approach of DPIA, as inferred from GDPR.




A data protection impact assessment overview derived from the French data protection authority (CNIL), attempts to provide to a generic methodology.

CNIL consolidates some of the steps proposed by working party 29 abstract methodology, without deviating. The CNIL implementation for DPIA as inferred from the scheme below can be summarized in the steps below :

## 1. Process Identification

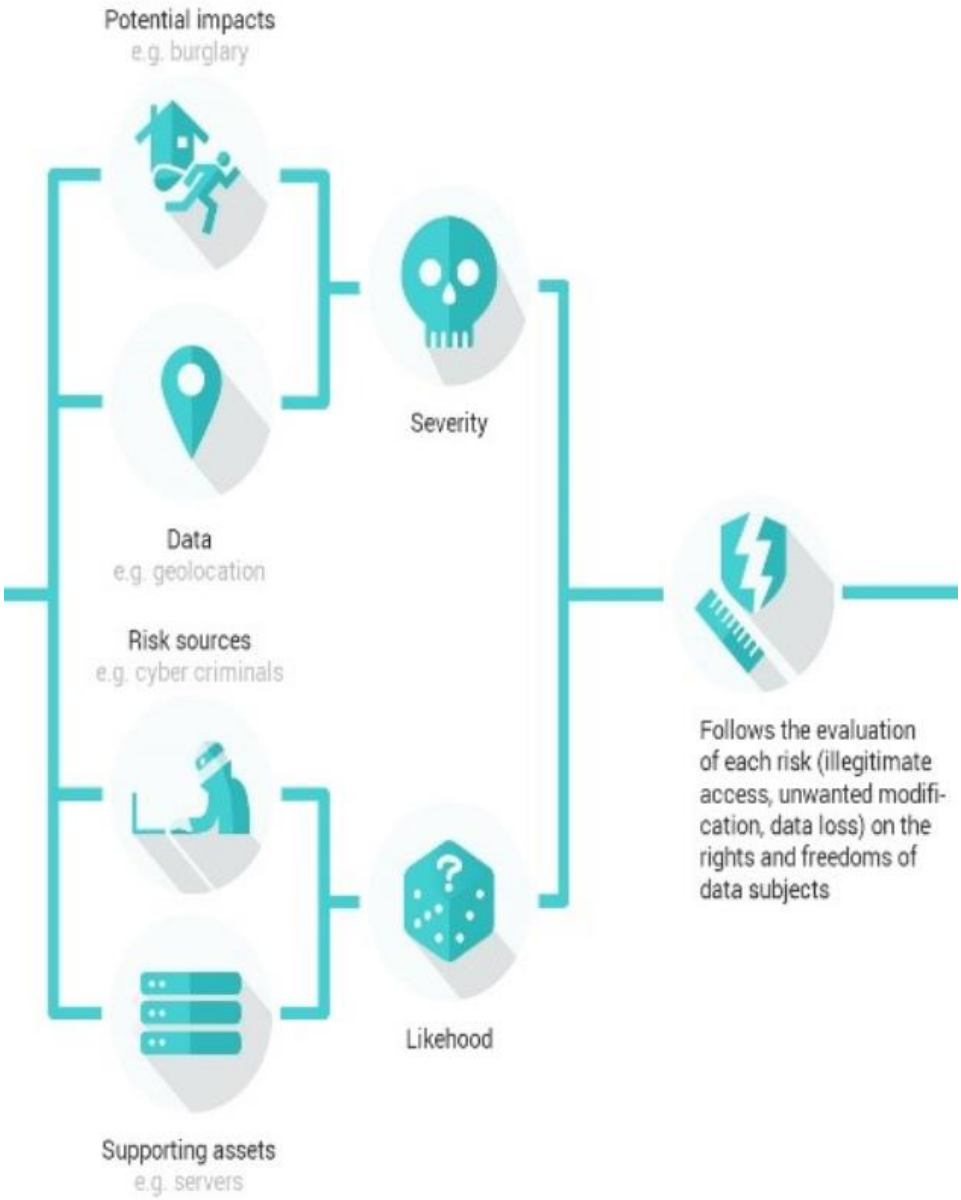
Describe the data processing from business aspect, the purpose, the involved data subjects ,the duration, types of data which will be processed , the assets on which the personal data reside during the processing, the potential recipients of the processing

## 2. Identify essential features of the processing and whether Dpia is required

Assess whether “high risk” condition exist using the extended list and the “rule” of the matches, provided by wp29.

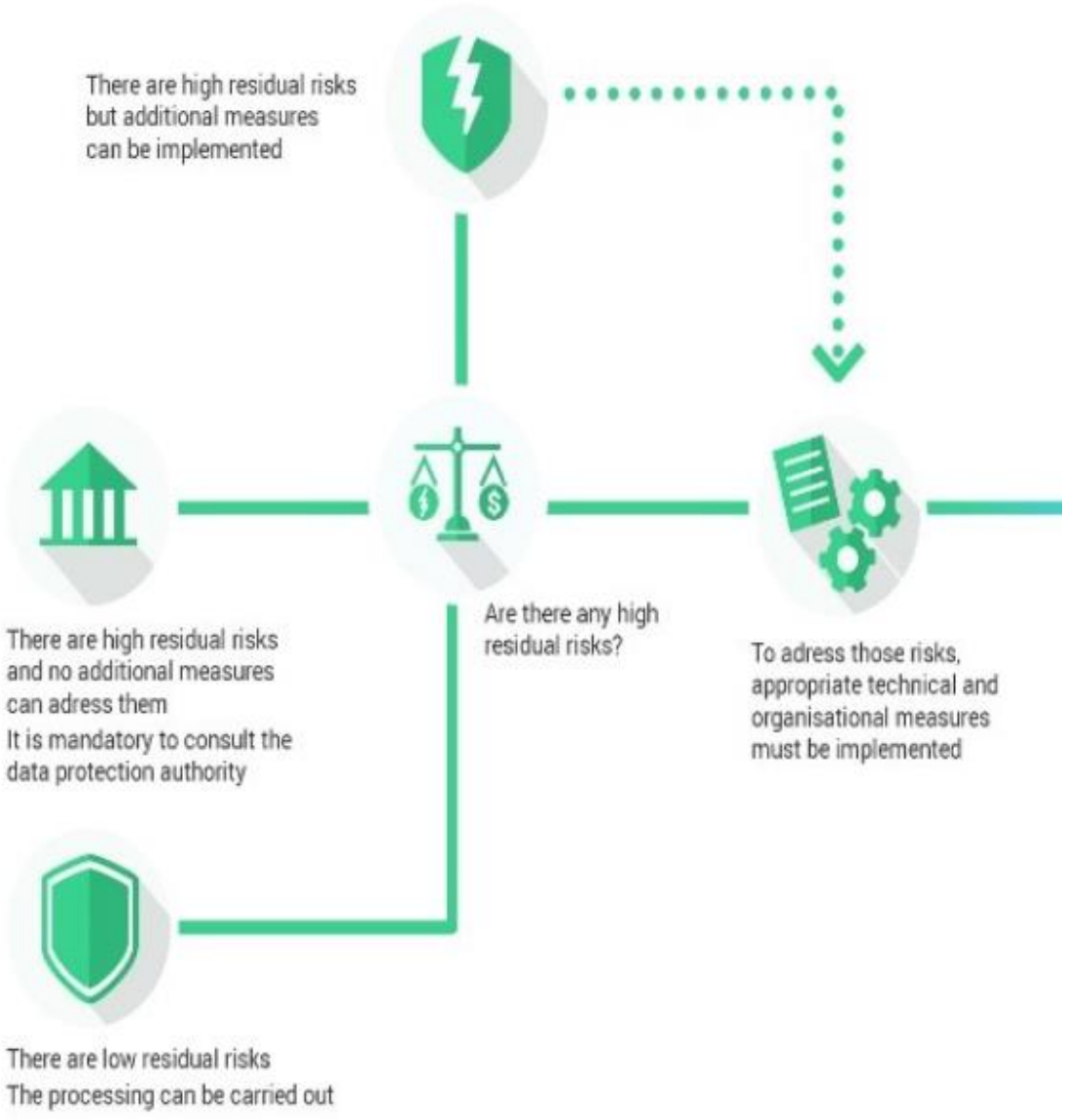

## 3. Risk evaluation

The assessment first establishes the context in which the processing is carried out, including its purpose and technical features. In addition to studying the fundamental principles, made up of the necessity and proportionality of the processing, each risk has to be analysed to evaluate its severity and likehood according to its potential impacts on the rights and freedoms of data subjects, the data processed, the risk sources and the supporting assets.




## 4. Address the risks

Once the risks have been identified, it should be determined if they are acceptable given the existing and planned technical and organizational measures. If it doesn't seem possible in regard of the foreseen measures, the data protection authority has to be consulted. In any case, it is mandatory to implement the planned controls before carrying out the processing.




A more detailed and procedural  methodology has been developed by british ICO, which meets the notion of a “handbook” as far as it is composed in a step-by-step format and includes the recording process of the activities conducted under the DPIA implementation.

It is additionally stated by ICO that the chosen format of the methodology intends to provide an effective way to integrate DPIA with the project management processes. This tension is very important because DPIA and GDPR compliance in general comes as an overlay procedure on the actual project management processes.

ICO’s methodology is summarized in 6 main stages :

## 1. Identification of the need to conduct a DPIA

During this stage, the data controller must describe what the project aims to achieve, what the benefits will be to the organization, to individuals and to other parties. In other words ICO prompts data controllers to describe the data processing in business terms and purposes of the processing, including, where applicable, the legitimate interest pursued by the controller. This first can be considered as an enriched description of Article 35(7)(a). Additionally in order to be able to depict in an optimum way the aforementioned characteristics of the project, ICO prompts the conductors of DPIA to attach or link any relevant documentation such a project proposal or a business analysis, which leaded to the generation or the alteration of a data processing.

Based on the project description, and the aspects of processing, data controllers must declare the reasons the need of conducting a DPIA emerged. The procedure proposed by ICO, was the methodology with the set of eight (8) questions, to which at least on confirmative answer indicates the need of a DPIA, described previously on the current document.

## 2. Describe the information flows

This stage requires from data controllers to describe how the personal data involved to the project will be collected, how they are going to be used, the means which will be used to collect them, process them and store them and finally their destruction/deletion procedure. It is of great importance to state during this stage how many individuals are likely to be affected by the processing and setup the information flows. Creating, attaching and referring to  flow diagrams will be very useful in order to explain the information flows and facilitate the DPIA review stages .

## 3. Identify the privacy and related risks

During this stage, Data Controllers must identify the key privacy risks and the associated compliance and corporate risks related to the processing. ICO prompts Data controllers to identify apart from risks to the rights and freedoms of data subjects (Article(35)(7)(c)) , the business risks for the organization in case of infringement of GDPR, derived from the privacy threats. ICO's methodology tends to pour a corporate and more applicable character in his suggestion and lead data controllers to a particular format of DPIA documentation.  The template below in extracted by ICO's documentation made publicly available .

| Privacy issue | Risk to individuals | Compliance risk | Associated organisation / corporate risk |
|---|---|---|---|
| | | | |

## 4. Identify privacy solutions

The fourth stage of ICO's proposed methodology, requires the description of the actions taken to reduce the risks. The template below is provided in order to help data controllers organize and document their activities.

| **Risk** | **Solution(s)** | **Result:** is the risk eliminated, reduced, or accepted? | **Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project? |
|---|---|---|---|
| | | | |

ICO chose four columns to depict all phases in chronological order and in time manner, in a way which clearly treats this stage as a traditional Risk Management workflow :

Column '**Risk**' : In this column all risks identified in the previous stage (stage three), are listed in order to help to the establishment of a complete mapping of the remedy measures.

Column '**Solution**' : This column hosts technical or organizational measures, which are applied to mitigate the risk present of the current row.

Column '**Result**' : This field hosts the outcome of the appliance of the measure, which exits in the 'Solution' and it may have only three values ( eliminated, reduced or accepted)

Column '**Evaluation**' : The purpose of this field is to record whether any additional measures must me taken in order to achieve the mitigation goal or they already applied ones have left no residual risk for the individuals.

It is inferred from the Risk management format ICO chose and the presence of the column "Evaluation", the continuous character of DPIA (Article 35(11)) and a shortcut to Aritcle 36 for prior consultation of the member state data protection authority .

If for example the 'Evaluation' column indicates significant residual risks even after applying technical and organizational measures, the project must never proceed without the data protection authority assessment.

## 5. Sign off and record the PIA outcomes

During this stage, ICO prompts controller to identify the privacy risk owners, which refers to the employees or the business entities/departments which are accountable for the risks. The notion of "**risk owner**", has never been mentioned in GDPR nor any complementary documentation, provided by wp29 or the EBDP. During this stage, the corresponding approved and taken measures for remedy must be recorded.

In case an alteration of the data processing or if the usage of a new technology take place, the threat probability to occur might be altered too, and new mitigation measure will have to applied. Assigning risk owners, facilitates the selective DPIA reviews and the targeted assessments on the rights and freedoms of the data subjects.

| Risk | Approved solution | Approved by |
|---|---|---|
| | | |

## 6. Integrate the PIA outcomes back into the project plan

The last stage of ICO methodology requires the role assignment and its recording for DPIA outcome integration with the project. Thus, british data protection authority requires data controllers to assign and document to employees or departments the implementation of the technical & organizational and the assignment (without naming it) of data protection officer, which will be the contact point for future privacy concerns. Here below, the relevant template provided for the documentation.

| Action to be taken | Date for completion of actions | Responsibility for action |
|---|---|---|
| | | |

| Contact point for future privacy concerns |
|---|
| |

## CONSULTATION

A very interesting perspective in ICO's methodology, is related to the notion of 'consultation'. Data controllers are prompted to record their consultation sources throughout the whole DPIA implementation, which will probably assist them to identify and address privacy risks or choose the technical and organizational measures. Information such as who they will be consulted internally or externally and how the will carry out the consultation and during which stages, must be documented.

**GDPR defines the minimum requirements for a DPIA in order to be valid and efficient. There are many approaches on how to conduct a DPIA, but there in no mandatory or suggested methodology. Many Data Protection Authorities have attempted to provide frameworks in order to facilitate data controllers implement DPIA, such the ones created by ICO,CNIL, and the german SDM.**

## CHAPTER 6. Who is responsible for carrying out a DPIA?

Throughout the Regulation, as also the WP29 guidelines, it is clearly stated that Data Controllers are responsible for carrying out a DPIA. Although, DPIA might be carried out by someone else, inside or outside the organization, the controller remains ultimately accountable about its conduction. In guidelines of WP29 , it is said that if the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information, thus staying in line with Article 28(3)(f).

There are certain cases where data processors, provide standard services no matter the Data Controller, and the processing they undertake is mainly the same in regular basis. Such examples might be software vendors (maintenance contracts included), cloud infrastructure providers, consulting services or any organization, which undertake to fulfill outsourced data processing according to data controller's needs.

Are these data processors responsible to for conducting a DPIA, at least a generic one, taking as granted that they might be well aware or even better aware than the data controller, of the risks which emerge form the subject processing for the rights and freedoms of the data subjects?

Is their compliance restricted under the scope of "assisting" data controller's DPIA ?

The answer to the aforementioned questions is derived indirectly both by :

- "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 " , where it is mentioned that a DPIA can also be useful for assessing the data protection impact of a technology product. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate.
- And by Article 28(3), where it is stated the sentence below :

"*With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions*."

This part of **Article 28, infers that data processors, do maintain mechanism to assess the compliance of a data processing activity with the regulation.**

Additionally any data processor, which deviates from the Data Controller's exact directions, is considered to be data controller also, for the current processing, and remains fully accountable to fulfill data subjects' rights.

All conditions above, create a perception that data processors must create a framework, If this is not a DPIA, which will grant them the ability to assess that all principles of Article 5 are not infringed during the processing, and to assist data controllers in their DPIA conduction.

## CHAPTER 7. METHODOLOGY DEPLOYMENT

Taking as granted all the aforementioned approaches developed by member state data protection authorities, wp29, EDPB and the decomposition of GDPR regulation articles conducted previously within the current document, it is a common understanding that an organization which begins its compliance effort, must improvise or follow practices which are based on assumptions .

To this point we will proceed with the deployment of a methodology, with the intention to be valuable and feasible to be followed, while being applicable and valid for a mainstream corporate environment.

The opinion communicated within the current document is that **an organization must implement a DPIA at least once, even if it considered that no process included in business operations is likely to result in a high risk to the rights and freedoms of natural persons.**

Lets describe at first the test environment on which we are about to deploy the methodology:

## Context /Key circumstances /Characteristics:

A mainstream organization, regardless the sector it belongs to, is defined by structure which includes some essential business entities (mostly met as distinct departments) which are indispensable for its operation, such as :

Accounting/payroll

Human Resources

IT/ IMS

Legal

Management

Finance

Quality / Internal Audit

and probably :Sector business entity 1

Sector business entity 2

Sector business entity 3

Sector business entity 4

- Each department fulfills a purpose and potentially conducts personal data processing.
- An organization maintains one or multiple information systems (eg. CRM, ERP, Document Management Software, Accounting/Payroll software) where personal data might reside.
- Each employee maintains a workstation and probably, accompanied by an LDAP software account.
- Data within the organization are stored in both physical and digital format.
- The organization either has an in-house DPO or has outsourced the DPO duties.

## Step 1 : DPIA PROJECT INITIATION

A) During the initial phase, the organization's management must officially present Data Protection Impact Assessment, as a part of organizations legal compliance project with GDPR regulation, and communicate the involvement of all employees to this purpose.

B) Additionally the organization's management must gather the team which will responsible for the DPIA conduction and choose the employee or the vendor which will fulfill the role of Data Protection Officer.

## Step 2: DPIA CONDUCTION TEAM MUST UNDERSTAND THE CONTEXT

During this phase the DPIA team gathered in Step 1 must :

A. Get fully involved and understand the organizations goals, the products or services
   The intention is to locate or predict the categories of data subjects that their Personal Identifiable Information (PII) will be processed.

B. Become aware of the organizations premises.

   - Is there exclusively a main site or alternative ones exist too ?
   - Are all premises located in EU?

C. Become aware of the company structure/business entities/departments of the organization

D. Get familiarized by the heads of the departments regarding the business purpose each of them fulfills.

## Step 3: LOCATE ALL THE BUSINESS ACTIVITIES WHICH INCLUDE INTERACTION WITH PERSONAL DATA

During this phase the DPIA conduction team becomes aware of all the business activities conducted by the departments. This phase includes interviews with the heads and the key users of each department and the intended outcome is to :

A. Identify the business activities which include personal data processing.

B. Record a detailed description in business terms.

C. Describe the information flows and, specifically, who collects what information from whom and how does the organization use the collected information, how is the information stored, secured, processed and distributed.

   It is extremely important to log during this phase the personal data format (digital or physical) and liaise if needed with the IT/MIS department for better mapping or understanding.

## Step 4 : MAPPING OF PERSONAL DATA PROCESSING ACTIVITIES IN COMPARISON WITH THE DATA PROTECTION PRINCIPLES

During this phase the DPIA conduction team must **per processing activity** :

A. Become aware or identify the purpose of personal data processing.

B. Identify whether personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

C. Identify whether personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

D. Identify whether the personal data processed are accurate and up to date and whether a process of erasure or rectification exists for inaccurate data.

E. Identify whether the personal data are processed for no longer than what is necessary for the purposes they have been collected and whether a process of permanent deletion or anonymization exists accordingly.

F. Become aware of the legal basis on which the processing is based (e.g consent, processing is necessary for the performance of a contract to which the data subject is party).

G. Does the processing involve personal data transfer to third countries or international organizations

H. Identify whether a logging mechanism exists for all the aforementioned .

## Step 5: CONSULTATION WITH STAKEHOLDERS

During this phase, the DPIA conduction team must seek the opinions of the data subjects or their representatives regarding :

A. Their perception about the risks emerging from the data processing

B. Which of their rights and their freedoms, think that might be compromised

C. In cases where the organization defines as legal basis of the processing the legitimate interests pursued by the controller, the data subjects must give their opinion on whether they believe their interests or fundamental rights and freedoms have been overridden, pursuant to Article 6.1.f

D. In cases where the organization defines as legal basis of the processing, the consent, the data subjects or their representatives, must give their opinion on whether the clearly understood the processing they consented to, and whether they feel that are any compelling circumstances that provoked them to provide their consent.

## Step 6: IDENTIFY THE EXISTENCE AND THE EFFICIENCY OF THE ORGANIZATIONAL MEASURES AND PROCEDURES ESTABLISHED IN ORDER TO FULFILL A POTENTIAL REQUEST DERIVED BY A DATA SUBJECT WHICH WISHES TO EXERCISE ANY OF ITS RIGHTS.

During this phase and for any business operation which includes personal data processing, the DPIA conduction team must verify :

A. The existence of “record of processing activities” and when and how is updated accordingly.

B. The existence of the procedure of providing information to the data subjects and if it fulfills the requirements of Articles 13,14 of GDPR

C. The existence and the efficiency of a procedure which allows the organization to provide information on whether or not personal data concerning him or her are

being processed. (It is indispensable for an organization in order to be able to comply with Articles 15-22 of GDPR)

## Step 7: IDENTIFY AND ADDRESS RISKS

During this phase the DPIA conduction team, must identify the privacy risks which exist as also their likelihood and their severity per business operation.

The risks must be divided to the **security oriented ones and the the organizational ones**.

**A.** For the security oriented ones, the list includes any threat which can exploit a vulnerability of the organization's infrastructure and lead to a data breach. These risks are related with the C.I.A (confidentiality, integrity, availability) model and are derived from traditional and state of art threats applicable to organizations infrastructure.

Identifying and addressing the risks of this nature, demands the conduction of a **security risk assessment** which includes under its scope all organization's information systems. In case the organization already has established and maintains an **ISMS** (Information Security Management System), there is no additional steps which need to be done for risk identification.

It is important to set clear that **there are no different security threats against Personal Identifiable Information (PII) and any other category of any piece of information, which needs to be protected.**

What has to be considered as different, is the fact that as far as the impact is related to the rights and freedoms of data subjects, there is no notion of "residual" of "accepted" risks, as so when a risk is not totally eliminated, the remedy action will lead to Data Protection Authority consultation or abort.

The DPIA conduction team, must cooperate with the security officer of the organization , members of the IT department and/or coordinate with external consultants in order to implement a security risk assessment with the particular characteristics described above

**B.** The organizational risks are derived from any compliance deviation with GDPR.

During this phase the DPIA conduction, will use the documentation created in **step 4** and **step 6** and compose a survey with:

- any missing implementation of procedures, policies

- any missing procedure or reporting tool used for data controllers accountability
- any faulty approach when choosing the legal basis of a data processing
- any infringement of the principle of “purpose limitation”
- any infringement of the principle of “storage limitation”
- any infringement of the principle of “data minimization”

During this phase representatives from many business entities/departments of the organization must participate and be consulted such as Accounting ,Human Resources and Internal Audit, in order to keep the DPIA conduction team aware of :

- Codes of conduct followed
- EU or member state legislations, which mandate the processing of personal data
- Active legal claims, which mandate the processing of personal data
- Any compelling condition, that the DPIA conduction team potentially is not aware of.

It is very important to understand, that organizational risks, as far as are mainly derived from compliance deviations, must be totally eliminated.

## Step 8: DPIA OUTCOME AND REMEDY ACTIONS

The DPIA conduction team creates an implementation plan of remedy actions, as emerged from the consolidation of the security risk assessment and the organizational measures assessment. The implementations plan will include :

- A detailed description of the remedy actions
- The responsible business entity or employee for each remedy action
- Time frame of the implementation
- External consultation, If needed.
- Reassessment dates.

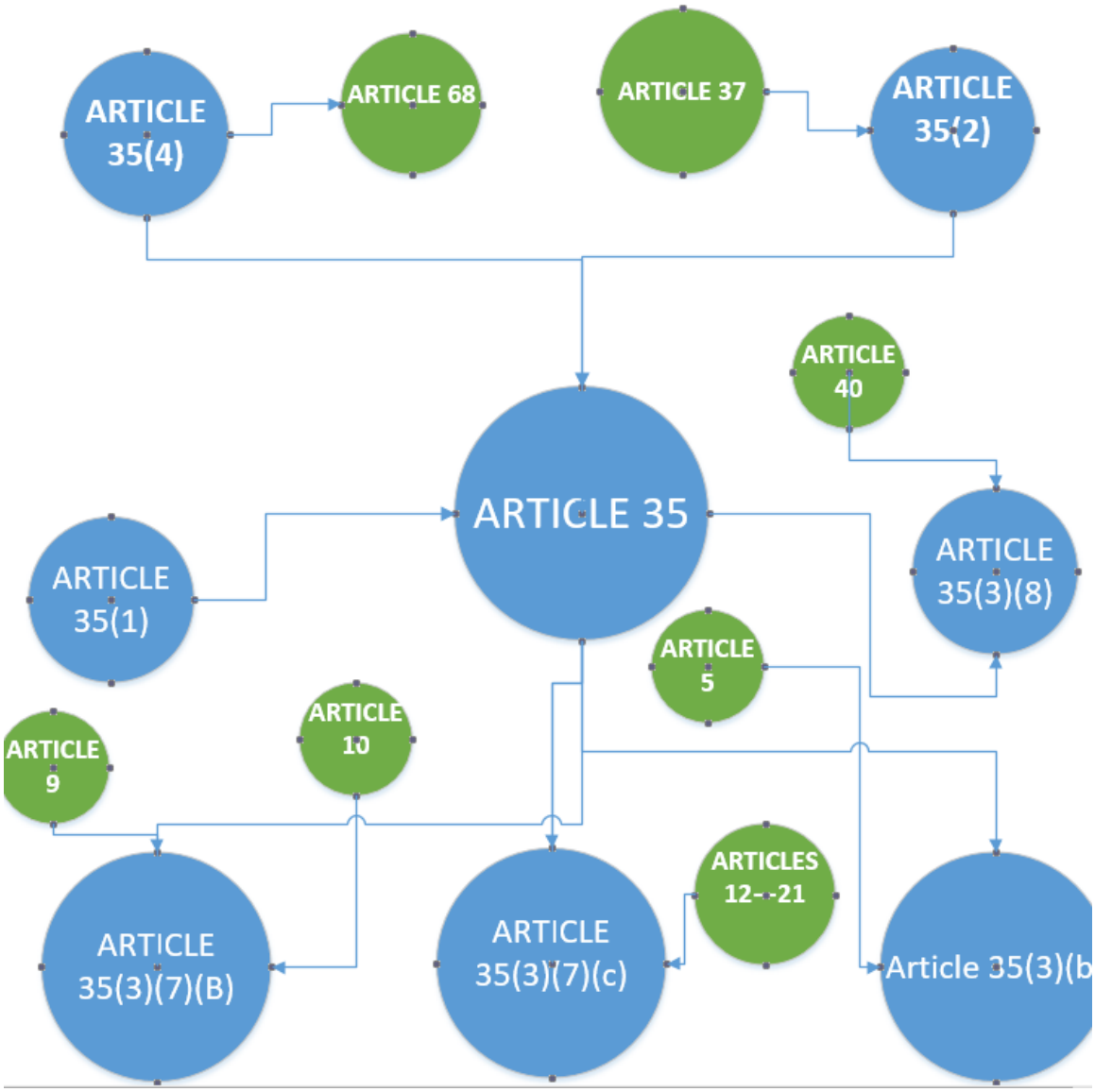
## CHAPTER 8. Conjectures, conclusions and comments on the body of the Regulation

- ✓ DPIA should be considered as a tool of reaching compliance with GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. It is explicitly mentioned in "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk" for the purposes of Regulation 2016/679 that DPIA "is a process for building and demonstrating compliance", as so it helps Data Controllers to prove their accountability, which is a new principal introduced in GDPR.

- ✓ In relation with the conjecture above it emerges that conducting a DPIA, even when it is not required prior to a processing operation it would be a good practice as it helps Data Controllers to organize their compliance attempt. DPIA as posed with its minimum requirements prompts conductors to ensure compliance with all GDPR principles and obligations which are bonded with them.

- ✓ Article 35 of the GDPR constitutes a "look- up" article to all essentials articles which can help an organization break down the whole Regulation and orchestrate their compliance project.

  A respective figure, is shown below :




- ✓ Article 35 of the GDPR, where the notion of DPIA is introduced mentions exclusively "Data Controllers" as potential conductors. The question as to whether a data processor bears the burden to conduct an independent DPIA when undertaking processing on behalf of a Controller remains open.

- ✓ Should be mandatory for software vendors, which provide tools designed in order to be used by data controllers and processors to assist them perform a part or completely a data processing activity, to conduct a generic DPIA on their products?

- ✓ The most important aspect in the phase of assessing whether a DPIA is required, it the determination on whether high risk circumstances emerge for the freedoms and the rights of the data subjects. Is there a recursive character in the definition of DPIA, as far as in order to assess whether "high risk" condition exist, the data controller must partially implement a DPIA ?

  It is elicited, although it is not mentioned directly in the Regulation, that a risk assessment with less extent must be performed by any Data Controller or Data Processor and prior to any data processing.

**Sources :**


https://free.dataguidance.com/laws/german-standard-data-protection-model-sdm/

https://www.cnil.fr/en/guidelines-DPIA

https://edpb.europa.eu/

- Opinion 05/2014 on Anonymisation Techniques
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679
- Guidelines on Data Protection Officers ('DPOs')
- Opinion 2/2017 on data processing at work
- Guidelines on Consent under Regulation 2016/679
- ICO: Pia-code of practice
- A step-by-step guide to privacy impact assessment(David Wright & Kush Wadhwa)