ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 248

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 4 April 2017

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Table of content

I. Introduction

Regulation 2016/679[1] (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA), as well as Directive 2016/680[2].

A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[3] (by assessing them and determining the measures to address them). DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[4]. In other words, a DPIA is a process for building and demonstrating compliance.

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Note: the term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.

---

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

[2] Article 27 of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, also states that a privacy impact assessment is needed for "*the processing is likely to result in a high risk to the rights and freedoms of natural persons*".

[3] The GDPR does not formally define the concept of a DPIA as such, but

- its minimal content is specified by Article 35(7) as follows:
  - "*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
  - *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
  - *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
  - *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*
- its meaning and role is clarified by recital 84 as follows: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk*".

[4] See also recital 84: "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*".

II. Scope of the Guidelines

These Guidelines take account of:

- the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 218[5];
- the WP29 Guidelines on Data Protection Officer 16/EN WP 243[6];
- the WP29 Opinion on Purpose limitation 13/EN WP 203[7];
- international standards[8].

Keeping in line with the risk-based approached embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory (Article 35(3)), the present guidelines firstly aim to clarify this notion and provide criteria for the lists to be adopted by DPAs under Article 35(4).

According to Article 70(1)(e), the European Data Protection Board (EDPB) will be able to issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. The purpose of this document is to anticipate such future work of the EDPB and therefore to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA.

These Guidelines also seek to promote the development of:

- a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
- a common EU list of processing operations for which a DPIA is not necessary (Article 35(5));
- common criteria on the methodology for carrying out a DPIA (Article 35(5));
- common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
- recommendations, where possible building on the experience gained in EU Member States.

[5] WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks adopted on 30 May 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

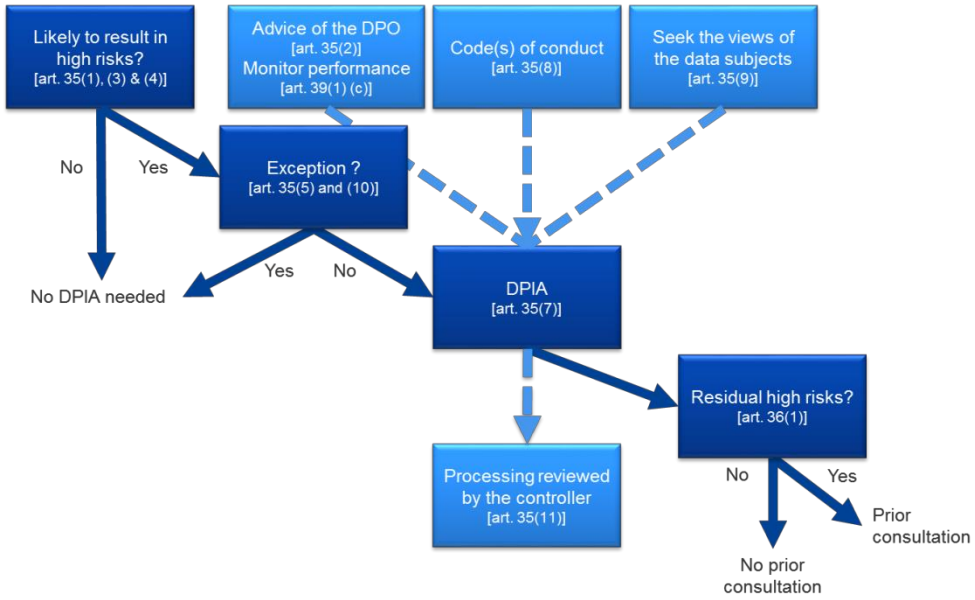
[6] WP29 Guidelines on Data Protection Officer 16/EN WP 243 Adopted on 13 December 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[7] WP29 Opinion 03/2013 on purpose limitation 13/EN WP 203Adopted on 2 April 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[8] e.g. ISO 31000:2009, *Risk management — Principles and guidelines*, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

III. DPIA: the Regulation explained

The following figure illustrates the basic principles related to the DPIA in the GDPR:



A. What does a DPIA address? A single processing operation or a set of similar processing operations.

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks*". Recital 92 adds that "*there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

This means that a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This might mean where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA.

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects.

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. 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. An example could be the relationship between manufacturers of smart meters and utility companies.

B. Which processing operations are subject to a DPIA?

This section describes when a DPIA is mandatory, when it is required because of likely high risk, and what needs to happen in the case of existing processing operations.

a) When is a DPIA mandatory? Where a processing is "*likely to result in a high risk*".

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where a processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced[9].

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law.

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing is "*likely to result in high risks*":

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*[10]*;*
- *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10*[11]*; or*
- *(c) a systematic monitoring of a publicly accessible area on a large scale*".

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processings[12], the following criteria should be considered:

1. Evaluation or scoring, including profiling and predicting, especially from *"aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements"* (recitals 71 and 91). Examples of

[9] See recitals 89, 91 and Article 35(1) and (3) for further examples.

[10] See recital 71: "*in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles*".

[11] See recital 75: "*where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures*".

[12] See e.g. recitals 75, 76, 92, 116.

this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))[13]. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).
4. Sensitive data[14]: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, 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 information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.
5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the

[13] The WP29 interprets "*systematic*" as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):

- occurring according to a system;
- pre-arranged, organised or methodical;
- taking place as part of a general plan for data collection;
- carried out as part of a strategy.

The WP29 interprets "*publicly accessible area*" as being any place open to any member of the public, for example a piazza, a shopping centre, a street or a public library.

[14] Nonetheless, if sensitive data are not processed systematically and on a large scale, their processing does not automatically present high risks for the rights and freedoms of data subjects. For example, a data controller organizing a corporate event, and would like to know therefore what kind of food his guests are allergic to, could process these sensitive data exceptionally and would not need to perform a DPIA. Similarly, processing of special categories of data by a medical doctor in a one-person practice should not be considered "*large scale*" (recital 91).

following factors, in particular, be considered when determining whether the processing is carried out on a large scale[15]:

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

6. Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject[16].
7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.
9. Data transfer across borders outside the European Union (recital 116), taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.
10. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processings performed in a public area that people passing by cannot avoid, or processings that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

The WP29 considers that 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. As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower

[15] See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
[16] See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.

level of risk, and processing operations which meet at least two of these criteria will require a DPIA. For example:

Examples of processing	Possible Relevant criteria	DPIA required?
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data - Data concerning vulnerable data subjects	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring - Innovative use or applying technological or organisational solutions	
A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	- Systematic monitoring - Data concerning vulnerable data subjects	
The gathering of public social media profiles data to be used by private companies generating profiles for contact directories.	- Evaluation or scoring - Data processed on a large scale	
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- (none)	Not necessarily
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on past purchases behaviour on certain parts of its website.	- Evaluation or scoring, but not systematic or extensive	

However, in some cases, a processing meeting only one of these criteria will require a DPIA. Conversely, if the controller believes that despite the fact that the processing meets at least two criteria, it is considered not to be "likely high risk", he has to thoroughly document the reasons for not carrying out a DPIA.

In addition, a data controller subject to the obligation to carry out the DPIA "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organisational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4))[17]. The criteria set out above can help supervisory authorities to constitute such a list, potentially with more specific content added in time if appropriate. For example, the processing of any type of

[17] In that context, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).

biometric data or that of children could also be considered as relevant for the development of a list pursuant to article 35(4).

b) When isn't a DPIA required? When the processing is not "*likely to result in a high risk*", or has already been authorized, or has a legal basis.

A DPIA is not required in the following cases:

- where the processing is not "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1));
- when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used (Article 35(1)[18]);
- where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis (Article 35(10))[19];
- where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required (Article 35(5)[20]). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, etc. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with the relevant requirements.

c) What about already existing processing operations? DPIAs are needed for those created after May 2018 or that change significantly.

The requirement to carry out a DPIA applies to processing operations meeting the criteria in Article 35 and initiated after the GPDR becomes applicable on 25 May 2018.

WP29 strongly recommends to carry out DPIAs for processing operations already underway prior to May 2018. In addition, where necessary, *"the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation"* (Article 35(11)[21]).

Moreover, this would be the case where a significant change to the processing operation has taken place[22] after May 2018, for example because a new technology has come into use or because personal

[18] "*A single assessment may address a set of similar processing operations that present similar high risks"*.

[19] Please note that where a DPIA was carried out at the stage of the proposal for the legal basis, it is likely to require a review before entry into operations, as the adopted legal basis may differ from the proposal in ways that affect the impact on privacy and data protection.

[20] To that extent, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).

[21] Article 35(10) explicitly excludes only the application of article 35 paragraphs 1 to 7.

[22] In terms of context, risks, purposes, personal data processed, recipients, data combinations, security measures and international transfers.

data is being used for different purpose. In cases like this, the processing in effect becomes a new data processing operation and could require a DPIA.

The DPIA should certainly be reviewed when there is a change of the risk presented by the processing operation (Article 35(11)).

Risks can change as a result of change to one of the components of the processing operation (data, supporting assets, risk sources, potential impacts, threats, etc.) or because the context of the processing evolves (purpose, functionalities, etc.). Data processing systems can evolve quickly and new vulnerabilities can arise. Therefore it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over longer time.

Finally, a DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, new categories of natural persons become vulnerable to discrimination or the data is intended to be transferred to data recipients located in a country which has left the EU.

As a matter of good practice, a DPIA should be continuously carried out on existing processing activities. However, it should be re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances. Such assessment is also recommended for data processing which have taken place before May 2018 and where therefore not subject to a DPIA, to make sure that 3 years after this date or sooner, depending on the context, the risks for the rights and freedoms are still mitigated.

C. How to carry out a DPIA?

a) At what moment should a DPIA be carried out? Prior to the processing.

The DPIA should be carried out "*prior to the processing*" (Articles 35(1) and 35(10), recitals 90 and 93). This is consistent with data protection by design and by default principles (Article 25 and recital 78).

The DPIA should be started as early as practical in the design of the processing operation even if some of the processing operations are still unknown. As the DPIA is updated throughout the lifecycle project, it will ensure that data protection and privacy are considered and promote the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. In some cases the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.

b) Who is obliged to carry out the DPIA? The data controller, with the DPO and the data processor(s)

The controller is responsible to ensure that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.

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.

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:

- those views could be sought through a variety of means, depending on the context (e.g. an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers);
- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the validation process;

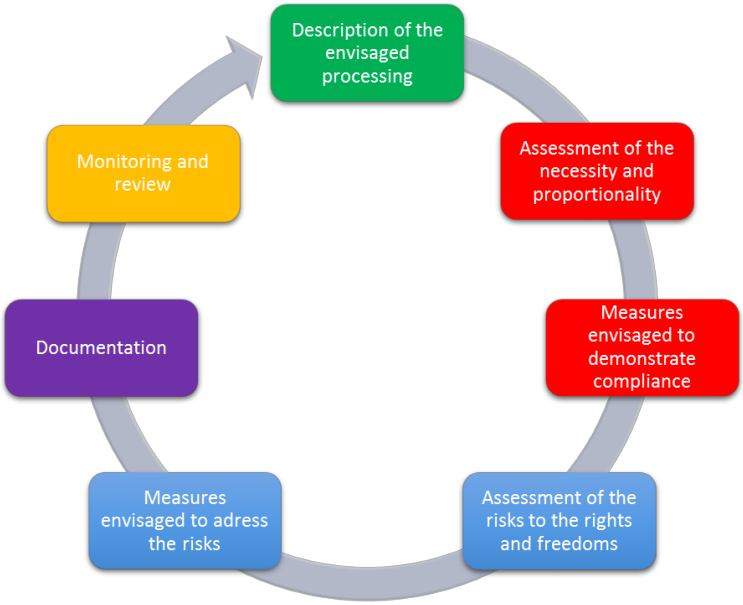
- where appropriate, it is recommended to seek the advice from independent experts of different professions[23] (lawyers, technicians, security experts, sociologists, ethics, etc.).
- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article 28(3)(f));
- the DPO could suggest that the controller carries out a DPIA on a specific processing operation, should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment, help to evaluate whether the residual risk is acceptable, and contribute to the development of knowledge specific to the data controller context;
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

c) What is the methodology to carry out a DPIA? Different methodologies but common criteria.

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- "*a description of the envisaged processing operations and the purposes of the processing*";
- "*an assessment of the necessity and proportionality of the processing*";
- "*an assessment of the risks to the rights and freedoms of data subjects*";
- "*the measures envisaged to*:
  - "*address the risks*";
  - "*demonstrate compliance with this Regulation*".

The following figure illustrates the generic iterative process for carrying out a DPIA[24]:



[23] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

[24] It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.

Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation.

All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. This opens the way for scalability, meaning that even a small data controller can design and implement a suitable DPIA.

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with well-defined components of risk management (e.g. ISO 31000[25]). In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following three processes, by:

- establishing the context: "*taking into account the nature, scope, context and purposes of the processing and the sources of the risk*";
- assessing the risks: "*assess the particular likelihood and severity of the high risk*";
- treating the risks: "*mitigating that risk*" and "*ensuring the protection of personal data*", and "*demonstrating compliance with this Regulation*".

Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, like it is done in certain fields (e.g. societal security), whereas risk management in some other fields (e.g. information security) is focused on the organization. A "*risk*" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. Article 35 refers to a likely high risk "*to the rights and freedoms of individuals*". As indicated in the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 218 (p. 4), the reference to "*the rights and freedoms*" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.

Different methodologies (see Annex 1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR.

In order to allow these different approaches to exist, whilst allowing controllers to comply with the GDPR, common criteria have been identified (see Annex 2). They clarify the basic requirements of the Regulation, but provide enough scope for different forms of implementation. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR.

[25] Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (see terms and definitions, and table of content, in the ISO 31000 preview: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectoral knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.

d) Should the DPIA be published? Yes, either in full or in part, and it must be communicated to the supervisory authority in case of prior consultation.

Publishing a DPIA is not a legal requirement of the GDPR. It is left upon the controller´s decision. However, data controllers should consider publishing their DPIA, or perhaps part of their DPIA. The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. It could even consist of just a summary of the DPIA's main findings.

Moreover, when a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be provided (Article 36(3)(e)).

D. When shall the supervisory authority be consulted? When residual risks are high

As explained above:

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1), see III.B.a). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;
- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures[26] envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be the storage of personal data on laptop computers with appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, etc.) in addition to existing policies (notice, consent, right of access, right to object, etc.).

In the laptop example above, the risks have been managed by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remains high) then the data controller must consult the supervisory authority.

An example of an unacceptable high residual risk includes where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome, and/or when it seems obvious that the risk will occur.

Whenever the data controller cannot find sufficient measures (i.e. when the residual risks are still high), consultation with the supervisory authority will be necessary.

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

[26] Including taking account of existing guidance from EDPB and supervisory authorities and taking account of the state of the art and the costs of implementation as prescribed by Article 35(1).

IV. Conclusions and recommendations

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processings. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

Article 24(1) sets out the basic responsibility of the controller in terms of complying with the GDPR: "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*".

The DPIA is a key part of complying with the Regulation where high risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.

Where a likely high risk processing is planned, the data controller must:

- choose a DPIA methodology (examples given in Annex 1) that satisfies the criteria in Annex 2, or specify and implement a systematic DPIA process that:
  - is compliant with the criteria in Annex 2;
  - is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;
  - involves the appropriate interested parties and define their responsibilities clearly (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, etc.);
- provide the DPIA report to the competent supervisory authority when required to do so;
- consult the supervisory authority when they have failed to determine sufficient measures to mitigate the high risks;
- periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation;
- document the decisions taken.

Annex 1 – Examples of existing EU DPIA frameworks

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). Such a framework can be bespoke to the data controller or common across a particular industry. Previously published frameworks developed by EU DPAs and EU sector-specific frameworks include (but are not limited to):

Examples of EU generic frameworks:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[27].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Examples of EU sector-specific frameworks:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[28].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[29]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

An international standard will also provide guidelines for methodologies used for carrying out a DPIA (ISO/IEC 29134[30]).

---

[27] Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.

[28] See also :

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[29] See also the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[30] ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and portability (Articles 15 and 20);
      - ☐ right to rectify, erase, object, restriction of processing (Article 16 to 19 and 21);
      - ☐ recipients;
      - ☐ processor(s) (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought (Article 35(9)).