When and how shall a privacy impact assessment be run?

A privacy impact assessment represents an obligation under the EU Data Protection Regulation in case of high risk data processing activities, but how and when shall it be done?

Updated on 18 October 2017 after the publication of the final version of the WP29 Guidelines on the data protection impact assessment

As part of the series of blog posts on the major changes introduced by the EU Data Protection Regulation, here is an article on how the privacy impact assessment, when it is mandatory and how it shall be run.

How can companies prove privacy compliance?

The EU Data Protection Regulation requires to put in place

> "***appropriate*** *technical and organisational measures to ensure a* ***level of security appropriate to the risk***"

Such requirement puts companies in a very hard position. In countries like Italy where privacy regulations have been prescribing so far very specific security obligations to be complied with, the EU Privacy Regulation represents a step back as it places the burden of identifying the appropriate security measures to the entity processing personal data (i.e. the data controller).

On the top of that, the principle of accountability even worsens the scenario since it places the burden of demonstrating privacy compliance on the entity that processes personal data. This is why the opinion of the Article 29 Working Party (WP29) on the so called "data protection impact assessment" (PIA or DPIA) defines the PIA as a

> "*process for building and demonstrating compliance*".

When is a privacy impact assessment necessary?

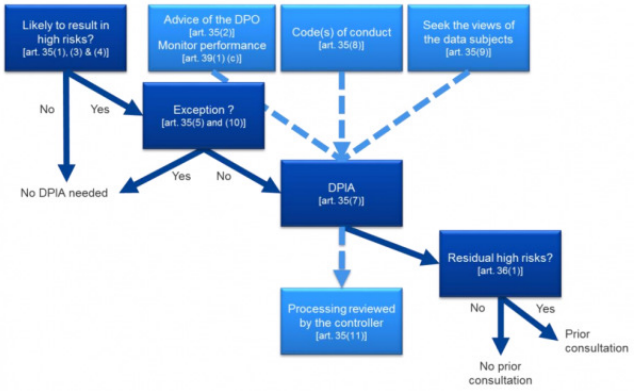
First of all, the European data protection authorities clarified in their opinion that

> "*carrying out a DPIA* ***is not mandatory for every processing operation****. Instead, a DPIA is only required where a type of processing is "****likely to result in a high risk to the rights and freedoms of natural persons****".*

This seems something that should not leave scope to potential misunderstandings. However, based on my experience, it often leads to different interpretations, just because the GDPR requires to implement "*appropriate technical and organisational security measures*".

On the contrary, the rationale behind the GDPR is to adopt a so called "*risk based approach*" i.e. the checks to be performed and measures to be implemented shall be based on the level of risk arising from a data processing activity. This is why it will be necessary **to run a data mapping activity and draft the registry of processing activities in order to identify the types of processing that may "*result in a high risk to the rights and freedoms*" of individuals** and as such require to run an assessment on the impact of the data processing activities on the protection of personal data (the so called "*data protection impact assessment*").

The chart below was published in the WP29 guidelines on the PIA and is a good summary of the process of assessment of scenarios when the PIA is required under the GDPR and what to do in each circumstance[0]



The identification of the need to run a PIA is relevant in particular when a new data processing technology is being introduced. As part of its opinion on the PIA, the WP29 provided a detailed list of high risk data processing activities that require to perform a privacy impact assessment, but this list is not in any case meant to be exhaustive:

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*" such as in cases when a financial institution [or also an insurance company] 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**. This last example is the one that is most relevant in my view since any e-commerce, gambling or other website has cookies and other tools that might perform such monitoring activity, but the need to perform a PIA will depend on the size of the database and level of profiling;
2. **Automated-decision making with legal or similar significant effect**: processing that aims at taking decisions on individuals producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*". For example, the processing may lead to the exclusion or discrimination against individuals, but also potentially **in case of automated systems of processing of applications for an insurance policy, a mortgage or a contract** which is the general practice;
3. **Systematic monitoring**: processing used to observe, monitor or control individuals, including data collected through "*a systematic monitoring of a publicly accessible area*". This scenario might be applicable for instance to **smart city technologies, CCTV systems, drones or Google Street View cars or the mere monitoring of employees**;
4. **Sensitive data**: this includes special categories of data (for example health related data or 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, as in case of eHealth projects and electronic health records. This criterion shall include
   - electronic communication data, location data, financial data (that might be used for payment fraud); and
   - information processed by an individual 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, but the WP29 recommends to consider the following factors,
   - 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; and
   - 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;
7. **Data concerning vulnerable data subjects**: the processing of this type of data can require a PIA 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 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 **patients**;
8. **Innovative use or applying technological or organisational solutions**, like combining use of finger print and face recognition for improved physical access control, etc. or Internet of Things technologies;
9. **Data transfer across borders outside the European Union**, 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. This means that **the mere adoption for instance of the Standard Contractual Clauses might not be per se sufficient** to ensure a compliant transfer of data outside of the EU;

10. When the processing in itself "***prevents data subjects from exercising a right or using a service or a contract***". This includes data processing operations performed in a public area that people passing by cannot avoid, or processing activities that aim at allowing, modifying or refusing individuals' 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.

According to the WP29, as a general principle, **processings that meet less than 2 criteria above may not require to perform a PIA**, but the matter shall be assessed on a case by case basis since even the meeting of one criteria might suffice. Also, the opinion of the WP29 **recommends to run a PIA when there is uncertainty as to whether it is required**. This risks to lead to the conclusion that companies might consider to run a data protection impact assessment, even when just one of the criteria above is satisfied in order to avoid the risk of challenges.

In any case, it should be considered that, even when the PIA is not necessary, the data processing operations shall be outlined in a record of processing activities that shall outline also the technical and organisational security measures that are put in place. And the data processing authorities shall publish a list of activities for which the PIA is required that might add further scenarios.

Does it apply only to the future data processing operations?

According to the opinion of the WP29, the obligation to run a PIA applies processing operations initiated after the GPDR becomes applicable on 25 May 2018. But the WP29 strongly **recommends to carry out PIAs 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***". This might be the case, among others, when

- either a new technology is used or collected data is used for a different purpose,
- or external factors, such as the increase of potential threats or risk sources, change;
- or changes in the organisation take place e.g. automated decisions become more significant or data is transferred outside the EU.

Indeed, the European privacy authorities emphasized that data controllers "*must continuously assess the risks created by their processing activities in order to identify when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons*". This means that it is necessary to put in place a procedure for **the review of both any new data processing activity and of any relevant change of the current data processing activities** which might also be the indirect result of changes to the organisational or societal context for the processing activity. As a consequence, a DPIA shall be "*reviewed and regularly re-assessed*" according to the WP29.

As a rule of thumb, the WP29 requires to reassess the PIA **at least every 3 years**, also in relation to data processing operations that were in place prior to May 2018.

A single PIA, multiple PIAs or PIAs for your customers?

The privacy impact assessment can relate to a single data processing activity, but also to a set of similar processing operations that present similar risks. In this respect, it is interesting that the WP29 identifies such latter scenario when, among others,

- A similar technology is going to be used by different entities. In such scenario, it is important to consider **the case when there are joint controllers** since the data protection impact assessment shall define "*which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects*". This is a frequent scenario in the case of Internet of Things technologies (e.g. a simple black box used for telematics insurance) where the technology supplier (in our example the provider of the black box) wants to be a data controller together with the insurance company; and
- A technology supplier wants to provide its hardware or software to its customers and wants to ease its adoption. Under such scenario, **the product/service provider could run the PIA on the technology and then its customers shall potentially need to perform a PIA only on its implementation**, if it triggers some changes. This is one of those scenarios when privacy compliance can lead to a competitive advantage since the time to market and the process of implementation of a technology that has already run a PIA would be considerably shorter.

How to do a data protection impact assessment?

When shall it be done?

Save for what stated above in relation to the existing data processing operations, the general rule is that the PIA shall be carried out **prior to the beginning of the data processing operations**. According to the WP29, as required in relation to the implementation of the privacy by design principle, the privacy impact assessment shall be performed during the design of the product/service.

This means that shall be initially performed and then updated or repeated throughout the whole development of the project, as a consequence for instance of choices relating to the technical and organisational measures to be put in place. And the WP29 has been clear in emphasising that the need to perform the PIA once the data processing operations have started **is not a valid reason to postpone it**.

Who shall do it?

The entity responsible to run the PIA is the data controller, but when the processing will be done in full or in part by a data processor, the latter shall assist the controller in the PIA and such assistance shall be contractually regulated in the data processing agreement.

Also, the GDPR requires that the controller must "*seek the views of data subjects or their representatives*" and this shall be done "*where appropriate*". This means that such step is not always mandatory, but the controller **shall document the reason why it decided not to perform it**.

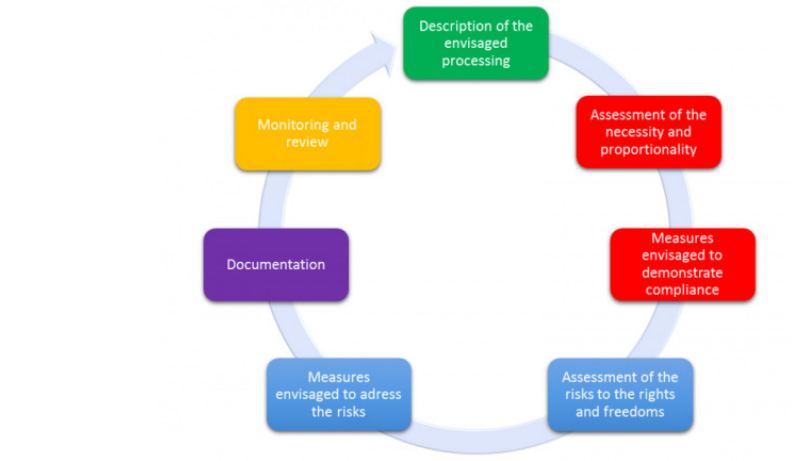
The WP29 also provide best practices in relation to, among others, the support from external consultants, such as lawyers and technicians, as well as the Data Protection Officer and the Chief Information Security Officer that shall assist during the PIA and propose its performance.

How shall it be done?

The privacy impact assessment requires under the GDPR to

1. provide a description of the envisaged processing operations and the purposes of the processing;
2. perform an assessment of the necessity and proportionality of the data processing operations e.g. with reference to the principle of data minimisation;
3. carry out an assessment of the risks to the rights and freedoms of data subjects; and
4. identify the measures envisaged to:
   - address the risks; and
   - demonstrate compliance with the GDPR.

The figure below was published as part of the opinion of the WP29 on the topic and represents and effective representation of the process



The PIA is essentially a tool to perform a risk management of data processing operations and is focused on 3 processes:

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

The WP29 refers to some data protection impact assessment methodologies that have already been developed, but also outlines that the GDPR is quite flexible on it. For this purpose, it provided a checklist of minimum contents of the PIA to assess whether the adopted methodology meets the criteria of the GDPR.

Does it need to be published?

According to the WP29, there is no obligation to publish the data protection impact assessment, but this might be a best practice to demonstrate accountability and transparency. In such case, it is possible to publish just a summary of the PIA, also in order to avoid the disclosure of confidential information and trade secrets.

When is a consultation with the data protection authority required?

The WP29 adopted a quite straight forward approach on the matter, limiting the need to perform a consultation with the competent privacy authority **only to cases when the PIA "*reveals high residual risks*"**.

Based on my experience, such scenario might occur when the implementation of the changes identified as part of the PIA cannot be performed since for instance they might either be excessively costly or require a long time of implementation. In this case, I can envisage the need to identify different routes to minimise the potential risks. However, it will ultimately be a responsibility of the data controller to ultimately prove whether such measures adequately limited the potential risks and therefore a consultation can be avoided.

The issue might be "*tricky*" since if a controller decides to initiate a consultation with the data protection authority, it means that it is not fully confident as to the measures implemented in order to minimise risks.

Finally, the consultation might be required under local laws. And this leaves the door open to additional local privacy law requirements which shall reduce harmonisation on privacy laws across the EU. This is the case for instance of Italy where, under current privacy laws, a prior consultation is required when the data processing activities trigger specific risks. And it is not fully clear whether such type of provisions will be fully repealed across the EU, as it was at least in the intention of the European legislator.

You may find also interesting my series of articles on the hottest topics of the European General Data Protection Regulation below

#1 Which companies shall care about it?

#2 Will fines be really massive?

#3 Did you run a privacy impact assessment?

#4 New risks for tech suppliers

#5 What changes with the one stop shop rule?

#6 How the new privacy data portability right impacts your industry

#7 What issues for Artificial Intelligence?

#8 How to get the best out of data?

#9 Are you able to monitor your suppliers, agents and shops?

#10 What liabilities for the data protection officer?

#11 Are you able to handle a data breach?

#12 Privacy by design, how to do it?

#13 How data on criminal convictions of employees become a privacy risk

#14 Red flag from privacy authorities on technologies at work

#15 Need a GDPR compliant data processing agreement?

#16 Is your customers' data protected from your employees?

#18 Data retention periods, an intrigued rebus under the GDPR

#19 Legitimate interest and privacy consent, how to use them?

If you found this article interesting, please share it on your favourite social media.

@GiulioCoraggio

WRITTEN BY GIULIO CORAGGIO

IT, gaming, privacy and commercial lawyer at the leading law firm DLA Piper. You can contact me via email at giulio.coraggio@gmail.com or giulio.coraggio@dlapiper.com or via phone at +39 334 688 1147.