VAN BAEL & BELLIS

Data protection impact assessment: More than just a compliance tool

Although it has been several years since the General Data Protection Regulation (GDPR) began applying throughout the European Union (EU), many organisations still hesitate to conduct a data protection impact assessment (DPIA). In light of this, Van Bael & Bellis' data protection team has compiled a list of questions that clients frequently ask, to clarify the concept itself and the benefits which a DPIA can bring to projects involving personal data.

1 | What is a data protection impact assessment (DPIA)?

A data protection impact assessment (***DPIA***) is a techno-legal process that helps organisations make better decisions on how to protect personal data and comply with the law. This process identifies, analyses and evaluates possible future consequences of the planned data processing operations of a project, and recommends the course of action to address the negative consequences.

DPIAs come in various shapes and forms, and exist in many countries. Typically, DPIAs are conducted before the start of high risk projects and may need to be revisited during a project's life cycle. DPIAs follow a fixed structure, and result in a report. They are often a collaborative effort that involves various internal (such as organisation's departments) and external (such as experts and even members of the public) stakeholders.

DPIAs were introduced in the European Union (***EU***) by the General Data Protection Regulation (***GDPR***) in 2018 and are now mandatory in certain circumstances in all EU Member States, as well as in Norway, Iceland, Liechtenstein, and the United Kingdom (***UK***). A related process, called privacy impact assessment (***PIA***), has been required and practised since a few decades in Australia, New Zealand, Canada and the United States, among other countries.

Are impact assessments specific only to data protection?

No. DPIAs are only one of the many types of impact assessment that exist in various areas and these include technology, environmental, regulatory, ethics or health impact assessments. DPIAs are also closely related to risk management.

Moreover, new types of impact assessment or conformity assessment have been constantly discussed, for example, for artificial intelligence (***AI***), algorithms or cybersecurity. Some of these types could become a legal obligation in the future and might overlap or dovetail with DPIAs to provide a fuller picture of potential consequences.

Finally, transfer impact assessment (***TIA***) is a popular name for a requirement to verify, case-by-case, if a third country to which personal data are transferred ensures an essentially equivalent level of protection in the absence of an adequacy decision.

2 | Why do I need to conduct a DPIA?

The short answer is that an organisation may need to conduct a DPIA because in specific situations it is a legal obligation. The law requires a DPIA to be done because there are fundamental rights at stake, especially the right to personal data protection.

The obligation to perform a DPIA is frequently criticised as constituting yet another regulatory burden, causing unnecessary expenditure and delays in the decision-making and implementation of projects. However, DPIAs can bring many benefits to an organisation. Performing a DPIA – even in situations where it is not mandatory – helps to comply with the law and demonstrate accountability.

Moreover, DPIAs help to rationalise decision-making processes, largely by offering best information available so that negative consequences can be avoided or minimised before they occur, thus saving resources. DPIAs can provide useful insights to

improve a planned project beyond its data protection aspects. Carrying out a DPIA also allows for the accommodation of diverse interests (such as technological development and data protection) and the gaining of public trust, as it shows that an organisation acted in a responsible manner (with due diligence), which can also avoid lawsuits and hence limit liability should something go wrong.

In addition, a DPIA can help with the practice of corporate social responsibility (***CSR***), implement UN Sustainable Development Goals (***SDG***) or comply with certified quality standards (for example, ISO 9001:2015 *Quality management systems*) or other legal requirements.

What happens if I don't do a DPIA or if I do it incorrectly?

If a DPIA is required by law, supervisory authorities may fine organisations up to EUR 10 million or 2% of the total worldwide annual turnover, whichever is higher, for a failure to carry out a DPIA either at all, or incorrectly. In 2022, for example, a supervisory authority fined a telecommunications company EUR 1.3 million for the poor quality of its DPIA. The organisation failed to correctly execute a mandatory step in the assessment of the necessity and proportionality of processing operations (Greek DPA Decision 4/2022).

In addition, organisations may always be ordered to repair damage should anybody suffer from the infringement of data protection law.

I have an accountability programme in my organisation. Do I still need to do a DPIA?

Yes. While accountability programmes typically focus on the overall approach of an organisation to their processing of personal data, a DPIA is narrowly focused on a single project.

3 | When do I need to do a DPIA?

As a rule, only projects involving processing operations that might result in high risk to the rights and freedoms of individuals require a DPIA.

The GDPR specifies which types of processing operations are deemed to be highly risky and hence require a DPIA. (*See our checklist in Annex to this Q&A*.) Indicators of high risk include the use of special categories of personal data, such as health-related data, the use of new technologies, or the monitoring and profiling of a large number of people. There might be some further requirements in each EU Member State.

Each organisation must itself determine whether to execute a DPIA for a given project. In case of doubt, it is better to carry one out. Even if a DPIA is not required by law, an organisation can always decide to perform a DPIA on its own initiative.

4 | How long does it take to do a DPIA?

The complexity and cost of a DPIA usually correspond to the complexity of the project.

Performing a DPIA can be a short and straightforward exercise if the project is fairly 'standard', even if it carries a high risk. In such a case, only a number of hours throughout the project may suffice for experienced assessors to conduct the DPIA. On the other hand, projects that involve novel processing activities or have a big business impact usually require investing more time and resources into a DPIA.

In any event, the resources required for a DPIA should be regarded as an investment, enhancing the quality and long-term viability of the project. Just as one would need to invest in a stability study before building a tall structure, one should invest in a DPIA before conducting an important data-related project (i.e., even where one is not mandatorily required under the law).

Do I still need to do a DPIA if my project is urgent?

An emergency does not absolve organisations from an obligation to conduct a DPIA prior to the processing operations. In 2022, for example, a supervisory authority fined an airport operator EUR 100,000 for multiple infringements of the GDPR, including the performance of a DPIA after the processing operations had already begun, as the airport operator had started using thermal imaging cameras during a public health crisis (Belgian DPA Decision 47/2022).

5 | When do I start a DPIA?

A DPIA is performed in the initial stages of a project so as to have a meaningful influence over its design. Without a DPIA, negative consequences might only come to light after a project has been implemented. Fixing the situation at such a late stage can be very costly and cause irreparable harm to an individual as well as reputational damage to an organisation.

6 | DPIA is about risk, but risk for whom?

DPIAs consider the consequences that a planned project could produce for individuals. Indeed, the GDPR imposes the legal obligation to assess the "risk to the rights and freedoms of natural persons".

By contrast, the assessment of consequences affecting organisations themselves, such as a risk of non-compliance with the law, belongs to a separate process. However, the DPIA can indirectly address such risks for an organisation, for instance by reducing the risk of receiving an administrative fine from a supervisory authority. Moreover, organisations can choose to integrate an assessment of the risk affecting the organisation into a DPIA.

Is a DPIA any different from a legal compliance check?

Yes. A DPIA does not only check if a project would comply with data protection laws, it also assesses what negative consequences this project could bring about for individuals.

What might be the negative consequences for individuals?

The possible negative consequences that people can suffer from the processing of personal data can be hard to predict. The GDPR gives some examples: "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage…". It is clear from these examples that many different types of consequences need to be considered, which is one of the reasons for performing a DPIA. Moreover, the GDPR adds that such consequences may also arise from evaluation of "personal aspects", for example, "analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (Recital 75).

Consequences might further include bodily harm (for example, a wrong medical treatment caused by inaccurate information), psychological harm (for example, harassment or bullying), reputational harm (for example, by a breach of confidential information) or economic effects (for example, not having access to goods or services).

7 | Who is involved in a DPIA?

A DPIA is a multidisciplinary, collaborative effort, engaging both internal and external stakeholders. The GDPR envisages a role for organisations (that assume the role of data controllers) to initiate a DPIA and be accountable for it. Data processors (those that process data on behalf of controllers), if any, might need to assist the controller and provide it with necessary information. Although it is typically not the role of the organisation's data protection officer (***DPO***) to perform a DPIA, the DPO should provide advice and monitor the performance of a DPIA.

Furthermore, people whose personal data is going to be processed in the future (data subjects) or their representatives can be consulted during a DPIA.

A supervisory authority, in turn, can play multiple roles, from providing support (guidelines, templates, training etc.), to prior consultation, or assessing the DPIA's quality (and imposing fines in case of deficiencies).

Do I have to do a DPIA myself?

Organisations can conduct a DPIA internally, for example, with help from the project leader, in-house lawyers or their data protection team. There is also dedicated software on the market to assist organisations with a DPIA.

Organisations can also choose to outsource the DPIA, in part or entirely, to an external assessor who is able to provide independent advice. If external counsel is involved, this has an additional benefit of granting legal privilege in accordance with applicable national laws.

However, organisations must make sure that their internal DPIA team or an external assessor has the necessary qualifications and experience, and that those involved are free from conflicts of interest.

Furthermore, assessors typically need to seek input from some specialists in the field, both internally and externally, for example experts in the fields of information technology (*IT*), information security, law, ethics or public relations (for example, for consultation with data subjects).

8 | What are the steps to perform a DPIA?

There are DPIA models available in many shapes and forms, including templates, questionnaires or software, originating from supervisory authorities, academia or private sector organisations. Their use is not mandatory, but if an organisation chooses to use one, it must verify that it contains all the mandatory requirements set out in the GDPR.

Once it is determined that a DPIA is required, the GDPR stipulates that it must contain at least the following elements:

I. A systematic description of data processing operations, which requires collecting the most complete information;

II. An assessment of proportionality and necessity of processing operations in relation to their purposes;

III. An assessment of the risks to the rights and freedoms of data subjects, in accordance with a method of an organisation's choice;

IV. Recommendations as to the measures to address negative consequences and demonstrate compliance with the law.

Where appropriate, a DPIA should also involve consultation with data subjects or their representatives. Such consultations are aimed at bringing new insights, and may range from surveys and interviews, to workshops, and their results should feed into a DPIA. Under no circumstances should such consultations bring about any negative consequences for their participants (for example, exploitation). However, a consultation might not be appropriate if there is little chance of any new insights, or if it is cost-inefficient or were to breach confidentiality. A choice not to consult stakeholders should be justified and documented.

The organisation can add further steps to a DPIA (for example, a quality control), as practicable. Eventually, a DPIA results in a report that serves to document the entire process and hence demonstrates accountability.

How do I assess a risk?

By way of example, the ISO 31000:2018 standard requires identifying risks, analysing them (determining their likelihood and severity), and evaluating them.

Who do I need to consult?

A consultation may involve individuals, non-governmental organisations (***NGOs***), trade unions, consumer organisations, lobby groups – at regional, national and/or EU level. It may also involve parents, or legal guardians who represent vulnerable people, for example, children.

Do I need to tell a supervisory authority about my DPIA?

If the outcome of a DPIA indicates that the project would result in a high risk in the absence of measures taken by organisations to mitigate the risk, the organisation must consult the competent supervisory authority.

9 | How do I protect confidential information within a DPIA?

Within a DPIA, for example while involving external stakeholders, confidential information – such as state or trade secrets, client-attorney communications, or personal data – must remain protected. Confidential information can be protected by the signing of non-disclosure agreements (***NDAs***), or redacting or summarising documents that reach the public.

Do I need to publish my DPIA report?

Although there is no such obligation, it is considered good practice to publish a DPIA report and relevant documentation to demonstrate compliance and accountability, even if redacted or summarised, with due respect for confidential information.

10 | I have done a DPIA. What now?

A DPIA finishes with a set of recommendations as to the measures needed – which could be of varied timeframes and priority – to address the negative consequences of a project and demonstrate compliance with the law. The outcome of a DPIA, including these recommendations, should be considered while designing the project. If the risks are too high, the project might need to be cancelled altogether. The DPIA report should be kept available to demonstrate accountability in case of an investigation or a claim.

At times, especially when there is a change of context – for example, new processing operations within a project or change of a risk level – an organisation might need to redo a DPIA, entirely or in part.

What measures are typically recommended?

The measures that are recommended depend on the risk that has been identified. For instance, if the DPIA shows that excessive categories of data are used, the recommendations can include restricting the data collection, or making some types of information optional. On the other hand, for an AI project where a DPIA established that the location data that were initially thought to be anonymous actually are personal data, recommendations can include implementing privacy-enhancing technologies (***PETs***), such as pseudonymisation or encryption.

Other typical recommendations include legal measures such as (re)drafting data protection notices, consent forms or data sharing agreements; or organisational measures, such as implementing the principle of data minimisation, data protection by default and by design, changing the geographical location of data storage or – simply – training the staff as appropriate.

VAN BAEL & BELLIS

BRUSSELS
Glaverbel Building
Chaussée de La Hulpe 166
B-1170 Brussels, Belgium
Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

GENEVA
26, Bd des Philosophes
CH-1205 Geneva
Switzerland
Phone: +41 (0)22 320 90 20
Fax: +41 (0)22 320 94 20

LONDON
5, Chancery Lane
EC4A 1BL London
United Kingdom
Phone: +44 (0)20 7406 1471

www.vbb.com

DPIA Checklist: What are the typical situations when a DPIA is required?

By way of example, an EU data protection advisory body offered, some years ago, a few generic suggestions for when to perform a DPIA, such as:

- ☐ Evaluation or scoring of individuals, including profiling
- ☐ Automated decision-making
- ☐ Systematic monitoring of people
- ☐ Processing special categories of personal data, for example health data, genetic or biometric data
- ☐ Data processed on a large scale
- ☐ Datasets that have been matched or combined
- ☐ Processing personal data concerning vulnerable people such as children or employees
- ☐ Innovative use of technological or organisational solutions
- ☐ Data transfer across borders outside the EU
- ☐ The processing of personal data which prevents people from exercising a right or using a service or a contract

This list is obviously non-exhaustive. Sometimes a single criterion suffices to trigger a DPIA. However, as new technologies emerge and the society develops, the need for a DPIA must be checked for each highly risky project involving personal data.

In addition, national supervisory authorities have adopted lists of situations where a DPIA is required in their jurisdiction. These national lists typically include situations such as:

- ☐ Use of data through a medical implant that could compromise a person's health
- ☐ Processing of genetic data
- ☐ Processing of biometric data to identify a person
- ☐ Migration of personal data between databases
- ☐ Employee monitoring
- ☐ Systematic processing and/or on a large scale of communication data (telephony, internet etc.), metadata, location data of a person which is not necessary for the requested service
- ☐ Processing data for scientific purposes
- ☐ Indirect data collection where it is not possible to fully inform the people
- ☐ Processing of data of very personal nature (poverty, unemployment etc.)
- ☐ Large-scale Internet of Things processing of data to make predictions about the behaviour of a person
- ☐ Whistleblowing schemes
- ☐ Big data analytics
- ☐ AI-based interactions with individuals
- ☐ Reward programs that generate profiles
- ☐ Video/audio analysis tools
- ☐ Fitness wearables and apps
- ☐ Use of non-EU vendors for processing sensitive data
- ☐ Investigations of which the person concerned is not aware
- ☐ Blacklists relating to infringements or bad payers
- ☐ Credit scoring
- ☐ Surveillance cameras
- ☐ Large-scale processing of human resources data with potential for significant effects on employees