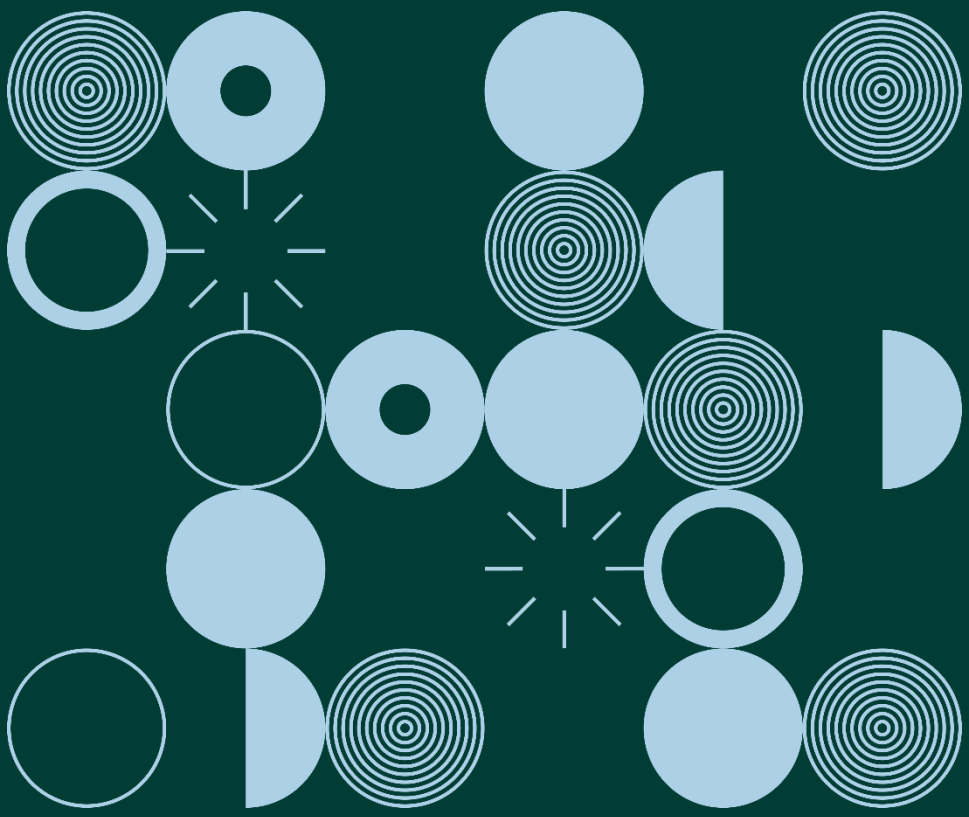
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Guide to Data Protection Impact Assessments (DPIAs)

October 2019



Contents

A Data Protection Impact Assessment (DPIA) is a way for you to systematically and comprehensively analyse the personal data processing you engage in or plan to engage in and help you identify and minimise data protection risks.

Controllers – those involved in determining how and why personal data are processed – need to undertake a DPIA for any processing that is '*likely to result in a high risk to individuals*', including some specified types of processing. The guidance below is aimed to assist you understand when and how to carry out a DPIA.

Key Points

- ☑ Under the General Data Protection Regulation (GDPR), DPIAs are mandatory for any high-risk processing projects.
- ☑ The DPIA process can help you to make informed decisions about the acceptability of data protection risks, and communicate effectively with the individuals whose personal data are concerned.
- ☑ The focus of a DPIA should be on potential harm to the rights or freedoms of data subjects, whether it is physical, material, or non-material.
- ☑ To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.
- ☑ Not all risks can be eliminated, but a DPIA can allow you to identify and mitigate data protection risks, plan for the implementation of any solutions to those risks, and assess the viability of a project at an early stage.
- ☑ If a DPIA does not identify safeguards which effectively mitigate any residual high risks, the Data Protection Commission (DPC) must be consulted.
- ☑ Good record-keeping during the DPIA process can allow you to demonstrate compliance with the GDPR and minimise risk of a new project creating legal difficulties.

What is a Data Protection Impact Assessment?

When a controller collects, stores, or uses (i.e. 'processes') personal data, the individuals whose data are processed are exposed to risks. These risks can range from personal data being stolen or inadvertently released and used by criminals to impersonate the individual, to worry being caused to individuals that their data will be used b for unknown purposes.

A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

This guidance assumes that a DPIA will be conducted for a defined project, rather than for an organisation's operations as a whole. A particular function of your organisation, or a programme of changes to your organisation's operations as a whole, may be viewed as a project.

What are the benefits of conducting a DPIA?

Conducting a DPIA can improve awareness of the data protection risks associated with a project. This will help to improve the design of your project and enhance your communication about data protection risks with relevant stakeholders. Some of the benefits of conducting a DPIA include:

- Ensuring and demonstrating that your organisation complies with the GDPR and avoids sanctions
- Inspiring confidence in the public by improving communications about data protection issues
- Ensuring your users/customers are not at risk of their data protection rights being violated
- Enabling your organisation to incorporate 'data protection by design' into new projects

- Reducing operation costs by optimising information flows within a project and eliminating unnecessary data collection and processing
- Reducing data protection related risks to your organisation
- Reducing the cost and disruption of data protection safeguards by integrating them into project design at an early stage

'Data protection by design' means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

'Data protection by default' means that service settings must be automatically data protection-friendly.

While long recommended as good practice, both of these principles are enshrined in law under Article 25 GDPR.

How do I know if a DPIA should be conducted?

Under the GDPR, a DPIA is mandatory where data processing "*is likely to result in a high risk to the rights and freedoms of natural persons*". This is particularly relevant when a new data processing technology is being introduced. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still good practice and a useful tool to help data controllers comply with data protection law.

In addition to the general conditions outlining when a DPIA is necessary, the DPC adopted the following list, pursuant to Article 35(4) GDPR, specifying certain types of processing for which a DPIA is mandatory:

1) Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4).

2) Profiling vulnerable persons including children to target marketing or online services at such persons.

3) Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects.

4) Systematically monitoring, tracking or observing individuals' location or behaviour.

5) Profiling individuals on a large-scale.

6) Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines.

7) Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines.

8) Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.

9) Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for difference purposes or by different controllers.

10) Large scale processing of personal data where the Data Protection Act 2018 requires "suitable and specific measures" to be taken in order to safeguard the fundamental rights and freedoms of individuals.

Further details on the obligation to complete a DPIA for the above sorts of data processing operations can be found in our guidance on 'Data Processing Operations which require a Data Protection Impact Assessment'.

The GDPR also provides further non-exhaustive examples of when data processing is 'likely to result in high risks', namely:

- "*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*"
- "*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*"
- "*A systematic monitoring of a publicly accessible area on a large scale*"

The Article 29 Working Party, consisting of the representatives from each data protection authority in the EU, adopted the following guidelines on DPIAs and whether

processing is likely to result in a high risk for the purposes of the GDPR - Guidelines on Data Protection Impact Assessment (DPIA). These guidelines were subsequently endorsed by the European Data Protection Board (EDPB), which replaced the Article 29 Working Party. In assessing whether processing is likely to result in a high risk those guidelines set forth the following criteria to consider:

Evaluation or Scoring

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 behaviour, location or movements*" (see Recitals 71 and 91 GDPR).

Examples of 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.

Automated Decision Making with Significant Effects

Automated decision making with legal or similar significant effect, or processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (see Article 35 (3)(a) GDPR).

For example, where 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.

Systematic Monitoring

Processing used to observe, monitor or control data subjects, including data collected through "*a systematic monitoring of a publicly accessible area*" (see Article 35 (3)(c) GDPR). 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 personal data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

Sensitive Personal Data

Sensitive data, this includes special categories of data as defined in Article 9 GDPR (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offenses. 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 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 considered as very intrusive.

Data Processed on a Large Scale

The GDPR does not define what constitutes large-scale, though Recital 91 GDPR provides some guidance. In any event, the WP29/EDPB guidelines recommend that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

1. The number of data subjects concerned, either as a specific number or as a proportion of the relevant population
2. The volume of data and/or the range of different data items being processed

3. The duration, or permanence, of the data processing activity
4. The geographical extent of the processing activity

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.

Data Concerning Vulnerable Data Subjects

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 (see Recital 75 GDPR).

For example, employees would often meet serious difficulties and suffer from a power imbalance where they sought to oppose to processing performed by their employer, when it is linked to human resources management. Similarly, children can't be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data.

This also concerns more vulnerable segments of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, the elderly, a patient, or in any case where a power imbalance in the relationship between the position of the data subject and the controller can be identified.

Innovation and Technology

Innovative use or applying technological or organisational solutions, like combining use of fingerprint and facial recognition data for improved physical access controls, etc. The GDPR makes it clear (see Article 35(1) and Recitals 89 and 91 GDPR) that use of a new technology can trigger the need to carry out a DPIA. This is because the use of a new 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.

International Transfers

Data transfer across borders outside the European Union (see 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.

Rights and Contractual Obligations

When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (see Article 22 and Recital 91 GDPR). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or reusing 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 Article 29 Working Party/EDPB guidelines consider that the more which 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 level of risk, and processing operations which meet at least two of these criteria will require a DPIA. If the controller believes that a processing operation which meets at least two of these criteria is not likely to be high risk, the controller should thoroughly document the reasons for not carrying out a DPIA.

When is a DPIA not required?

A DPIA is generally 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) GDPR)
- When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIAs have been carried out. In such cases, results of a DPIA for similar processing can be used (Article 35(1) GDPR)
- Where a processing operation has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a general impact assessment, according to the standards of the GDPR, has already been carried out in the context of the adoption of that legal basis (Article 35(10) GDPR)
- 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) GDPR). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorisations, compliance rules, etc. In such cases, and subject to reassessment 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.

Do DPIAs have to be renewed for existing processing operations?

The GDPR became effective from the 25 May 2018, and the Article 29 Working Party/EDPB guidelines specifically noted that the requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

However, a DPIA is not needed for processing operations that have already, pre-GDPR, been checked by a supervisory authority or the data protection official (in accordance with Article 20 of Directive 95/46/EC), and that are performed in a way that has not changed since the prior checking.

Therefore, any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior assessment and which are likely to result in a high risk should be subject to a DPIA.

New DPIAs or reviews of DPIAs for existing processing that commenced before the 25 May 2018 may be required after that date in the following circumstances:

- Where a significant change to the processing operation has taken place after the GDPR takes effect. For example, when a new technology comes into use, or when data is being used for a different purpose. In these cases the processing is effectively a new operation and could require a DPIA.
- When there is a change of the risk presented by the processing operation. The risks and level of risk can change as a result of a change to one of the components of the processing operation (data, supporting assets, risk sources, etc.), or because the context of the processing evolves (purpose, functionalities, etc.). Data processing systems can evolve over time, and new threats and vulnerabilities can arise.
- 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 reviewed and regularly re-assessed. Therefore, even where a new DPIA was not strictly required for an existing operation on the commencement of the GDPR, it will be necessary, at the appropriate

time, for the controller to conduct such a DPIA as part of its general accountability obligations.

When in a project lifecycle should a DPIA be conducted?

The DPIA should be carried out 'prior to the processing' (see Articles 35(1) and 35(10), and Recitals 90 and 93 GDPR). It is generally good practice to carry out a DPIA as early as practical in the design of the processing operation. It may not be possible to conduct a DPIA at the very inception of the project, as project goals and some understanding of how the project will operate must be identified before it will be possible to assess the data protection risks involved.

For some projects, the DPIA may need to be a continuous process, and be updated as the project moves forward. The fact that a DPIA may need to be updated once processing has actually started is not a valid reason for postponing or not carrying out a DPIA.

Who should be involved in conducting the DPIA?

The data controller is responsible for ensuring the DPIA is carried out. It may be delegated to someone else, inside or outside the organisation, but the data controller is ultimately accountable.

The DPIA should be driven by people with appropriate expertise and knowledge of the project in question, normally the project team. If your organisation does not possess sufficient expertise and experience internally, or if a particular project is likely to hold a very high level of risk or affect a very large number of people, you may consider bringing in external specialists to consult on or to carry out the DPIA.

A wide internal consultation process can benefit the DPIA, as some data protection risks will only be apparent to individuals working on specific aspects of the project. It will also allow you to gain feedback from those whose work will be affected by the project after implementation, such as engineers, designers and developers, who will have a practical knowledge of the operations. Involving your organisations public relations team will allow for effective communication of the DPIA's outcomes to external stakeholders.

Under Article 35(2) GDPR, it is necessary for any controller with a designated Data Protection Officer (DPO) to seek the advice of the DPO, when carrying out a DPIA. This advice and the decisions taken should be documented as a part of the DPIA process. If a data processor is involved in the processing, the data processor should assist with the DPIA and provide any necessary information.

The DPO is a designated person appointed by an organisation to advise on data protection practices within the organisation. The DPO can be a staff member or an external service provider. Under the GDPR, appointment of a DPO is mandatory in the following circumstances:

- ☐ For public bodies carrying out data processing, except for courts acting in their judicial capacity;
- ☐ If the core activities of the organisation consist of data processing which, by virtue of their scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- ☐ Where the core activities of the organisation consist of processing on a large scale of special categories of data as outlined in Article 9 or personal data relating to criminal convictions as outlined in Article 10 of the GDPR.

The controller is bound to 'seek the views of data subjects or their representatives' (per Article 35(9) GDPR), 'where appropriate' in carrying out the DPIA. In some cases, the data subjects may be people within the organisation. Seeking the views of data subjects will allow the controller to understand the concerns of those who may be affected, and to improve transparency by making individuals aware of how their data will be used.

The views of data subjects can be sought through a variety of means, depending on the context. Staff could be consulted through a trade union; customers could be consulted by means of a survey. If the controller's final decision differs from the views of data subjects, the reasons should be recorded as a part of the DPIA. If the controller does not feel it appropriate to seek the views of data subjects, the justification for this should be documented.

What steps are involved in carrying out a DPIA?

The GDPR sets out the following minimum features which should be present in a DPIA (see Article 35(7) and Recitals 84 and 90 GDPR):

- ☐ "*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*"; and
    - "*demonstrate compliance with [the GDPR]*".

The GDPR presents a broad, generic framework for designing and carrying out a DPIA. This allows for scalability, so even the smallest controllers can design and implement a DPIA; as well as for flexibility, so the controller can determine the precise structure and form of the DPIA, allowing it to fit with existing working practices.

Key stages of a successful DPIA

The GDPR does not prescribe the exact process for carrying out a DPIA beyond the minimum features outlined above, allowing for flexibility and scalability in line with your organisation's needs. Although there is no one prescribed approach to take, the following steps can guide you through the process:

1. Identifying whether a DPIA is required;
2. Defining the characteristics of the project to enable an assessment of the risks to take place;
3. Identifying data protection and related risks;
4. Identifying data protection solutions to reduce or eliminate the risks;
5. Signing off on the outcomes of the DPIA;
6. Integrating data protection solutions into the project.

1. Identifying whether a DPIA is required

You can use the steps described in the above section 'How do I know if a DPIA should be conducted?' to assess if you need to perform a DPIA. This should take place as early as practicable in the lifecycle of the project. You will also need to identify the resources needed, the individuals who will be involved, and the timeframe of the DPIA process.

As the nature and operational implications for data privacy of a project may not be apparent at an early stage in the planning, the DPIA may need to be an ongoing process, and may need to be reviewed or repeated as the project moves forward.

2. Describing the information flows

At an early point in the DPIA project, you should identify how it is intended to collect, store, use and delete personal data as part of the project. This exercise should also identify what kinds of personal data will be used as part of the project and who will have access to the personal data.

The aim of this step is to get an early understanding of how personal data will be used as part of a project at each step along the process. This is crucial to being able to recognise the data privacy risks which may be posed by a project and to identifying what means might be used to mitigate those risks.

You should consider if any new personal data will be generated by the project, and include it in your record of this stage. For example, a project involving the processing of psychometric tests might take one type of personal data (the answers to psychometric test questions) and process it to another (a psychometric profile). This new type of personal data is different in character, and so recording it separately in your map of data flows will help to ensure that its special characteristics are taken account of later in the DPIA process.

This part of the DPIA will often mirror other elements of your project design process, such as a general scoping exercise to identify how the project will be carried out, and can be integrated with such a scoping exercise. Paying attention in the design of a project to how personal data will be used as part of the project may also yield efficiency

benefits for your organisation by assisting you in streamlining processes for handling personal data.

At this stage of the DPIA process, you should consult with internal stakeholders with a view to identifying the technical aspects of data collection, storage and processing, and how the different elements of the project will fit together in operation. You may also want to consult with external partners, who may be engaged by your organisation as a data processor, or to whom personal data might be disclosed as part of a project.

This exercise should be documented using whatever means are most suitable for your organisation and the project concerned. Using visual aids, such as flow charts, to document how personal data will be used as part of a project can assist in identifying potential data privacy risks. This may also help with internal communication by better allowing the project team and others in your organisation to understand the design of the project.

3. Identifying data protection and related risks

This stage involves examining the project design to assess what data protection issues arise in the project, and to identify any data protection risks it may expose individuals to. There are a range of different ways that an individual's data protection rights can be compromised or put at risk by a new project. The types of risk range from the risk of causing distress, upset or inconvenience to risks of financial loss or physical harm.

This step should build upon work done at previous stages of the DPIA. The responses to the criteria laid out in the above section 'How do I know if a DPIA should be conducted?' should act as a guide to the risks which may be present. The map of information flows generated in stage 2 may help you to identify particular weak spots, where general risks are likely to be particularly acute, or which might give rise to specific risks.

Examples of the types of risks that you should be alert for at this stage of the DPIA process are outlined below. You should also examine sector-specific guidance which may be provided by regulators or industry groups in your area of operations, which can highlight types of risk which may be relevant for your organisation or project.

You should take note of the magnitude of the risks identified, having regard to both the likelihood of a risk manifesting itself, and its impact. In assessing the severity of the risk, it is important to bear in mind the sensitivity of the personal data to be processed as part of the project, the number of people likely to be affected by any of the risks identified, and how they might be affected.

You should keep a record of all risks identified at this stage. This will assist later on in the DPIA process in creating solutions to avoid or reduce those risks. Record-keeping may be especially important in the event of an investigation or audit by the DPC. Good record-keeping may help to demonstrate how your organisation complied with its obligations under the GDPR.

This identification exercise should be carried out relatively early in the project design, as the sooner that risks can be identified, the easier and cheaper it will be to mitigate them. However, it is not a once-and-for-all exercise; you should keep the project design under review throughout the DPIA process to monitor the emergence of any new risks, which may occur by reason of a change to the design or scope of the project, and to assist in assessing which risk reduction techniques work.

Your organisation can choose the risk management approach that best suits your existing project management process. Similar tools or methods to those you use for identifying other regulatory or commercial risks as part of your project management process could be used or adapted to assess the data protection risks involved in a project. The key point is to ensure that a methodological approach to identifying the data protection risks to the rights or freedoms of data subjects is adopted, and that records are kept of this process, and of all the risks identified.

Your organisation may wish to maintain a data protection risk register to describe the risks associated with a project and assess their likelihood and impact. You can then go back to the register in the event of any changes to the project, to make note of any steps taken to mitigate risk, or any additional risks that emerge. This can be incorporated into an existing risk register if one exists for the project.

> A data protection risk register is a master document that is used to record information about data protection risks which have been identified in relation to a particular project,

as well as an analysis of risk severity and evaluations of the possible solutions to be applied. The data protection risk register should be updated as the project progresses, to reflect any solutions or new risks which have been identified.

Small scale projects may adopt a relatively informal approach to risk. You can still use a data protection risk register in such cases, but with the entries reflecting the less formal approach adopted.

Potential Risks to Data Subjects

The following is an indicative, non-exhaustive list of the types of risks to the rights and freedoms of data subjects which you may need to consider when carrying out your DPIA:

- ☐ Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- ☐ Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- ☐ Breach of data held electronically by 'hackers'.
- ☐ Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- ☐ Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- ☐ Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- ☐ Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- ☐ Personal data being used for automated decision making may be seen as excessively intrusive.
- ☐ Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.

- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

4. Identifying and evaluating data protection solutions

This stage follows on from the identification of data protection risks at stage 3, with the aim of minimising the data privacy risk associated with the project, insofar as possible. In almost all cases, it will not be possible to eliminate data protection risks completely, but the aim of this stage is to balance those risks against the aims of the project, to ensure that any risks that are accepted are proportionate to the outcomes of the project. However, under GDPR, if there are remaining high risks, then you will need to consult with the Data Protection Commission, as described below.

During this stage, you should try to identify risk mitigations measures to reduce the impact of the project on data protection. These are measures which may be taken to reduce the likelihood or severity of data protection risks being realised. You should do this by looking at each of the risks identified as part of the previous stage in the DPIA process and seeking to address it individually, or as part of a privacy solution which may address a number of risks together.

In some cases, risk mitigation measures may be able to eliminate some types of risk, for example by abandoning unnecessary parts of a project which create unique risks. In others, risk mitigation measures may simply mitigate against risk or reduce the

significance of data breaches, for example by adopting pseudonymisation to reduce the risk of identification of data subjects.

The nature of these measures will depend on the types of risk that have been identified, and the aims of the project. You should keep a full record of the process, to document any risk mitigation measures which have been identified, and which risks they were intended to address, as well as any risks which have been accepted. This can be included as part of a data protection risks register as described above.

Equally, in assessing whether a particular risk mitigation measure should be pursued, it is necessary to weigh up the costs and benefits of each solution. For example, anonymising data may help to prevent the risk of data relating to an identifiable person being accidentally disclosed to a third party, but it is likely to cost the organisation money to put an anonymisation system in place, and it may prevent some of the goals of the project from being realised (if those goals depend on processing information about identified individuals).

Every project will have its own unique circumstances and risk profile, so there is no 'one size fits all' set of risk mitigation measures which may be adopted. However, the following are examples of risk mitigation measures, some of which may be applied in a range of different scenarios:

- Deciding not to collect or store particular types of personal data.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.
- Creating protocols for the handling of personal data within the project, and ensuring that all relevant staff are trained in operating under the protocol.

- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of personal data.
- Assessing the need for new IT systems to safely process and store the personal data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their personal data will be used.
- Providing a contact point for individuals to raise any concerns they may have with your organisation.
- If you are using external data processors, selecting appropriately experienced processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

In most cases, there are some data protection risks which cannot be eliminated or reduced. These risks can be accepted if they are proportionate to the outcomes that will be achieved by proceeding with the project notwithstanding the risk. Any decisions to accept data protection risks should be recorded in the data protection risk register, or otherwise in accordance with your project management process.

At this stage, you should also ensure that the project will be in compliance with other aspects of data protection law. In particular, you should consider whether the project complies with the data protection principles, and ensuring that you have a valid legal basis for processing personal data.

5. Signing off and recording the DPIA outcomes

The primary aim of conducting a DPIA is to identify and minimise the data protection risks involved in a project. As has been emphasised throughout this guide, keeping a record of all steps taken as part of the DPIA will help ensure that the process is completed thoroughly, reassure stakeholders that all data protection risks have been considered, and enable the controller to demonstrate their compliance with their data protection obligations, in line with the principle of accountability.

This written record should also form that basis of putting into effect any risk mitigation measures which have been identified, and can be used to check off the implementation of each measure.

There is no requirement to produce a final DPIA report but it is good practice to do so. This report should bring together, in summary form, the record keeping from each stage of the DPIA process and note the conclusions from each step of the process. It should also include an overview of the project, explaining why it was undertaken and how it will impact on data protection. It should describe the process adopted in conducting the DPIA, and set out the data protection risks and solutions which were identified as part of the process.

Your organisation may decide to publish the DPIA report or a summary of it. The decision of whether or not to publish the report will probably have a bearing on how much detailed information is put into the report, as it may not be appropriate to publish commercially sensitive information or information containing too much detail about security vulnerabilities which have been identified.

A DPIA does not necessarily require a formal signing-off process, but your organisation may require it, particularly if it recommends significant changes to the nature of a project, or if it recommends accepting significant risks.

If the data protection risks which have been identified are not capable of mitigation consistent with the goals of a project, and it would not be proportionate to accept them, this stage should be used for re-evaluating the viability of the project. In such

circumstances, an organisation may decide to either change the goals of a project to allow for mitigation of data protection risks, or abandon the project altogether.

6. Integrating the DPIA outcomes back into the project plan

Once it has been signed off, it is necessary to put the findings of the DPIA into action by integrating any necessary changes into the plans for the project. The earlier the DPIA can be completed, the easier it will be to give effect to any risk mitigation measures, but as the DPIA will not normally be completed until the project has already progressed somewhat in the planning stages, it will normally be necessary to adjust plans to give effect to risk mitigation measures identified.

As part of the implementation of the DPIA, you should keep data protection issues under review. In particular, you should assess whether the risk mitigation measures implemented are having the intended effect of mitigating risks to the rights and freedoms of data subjects. Additionally, if the project aims change or expand over its lifetime, it may be necessary to assess whether a further DPIA is required to assess the effect of the changes on the data protection risks identified. Such a review can be built into your organisation's existing procedures.

Should the Data Protection Commission be consulted on completion of the DPIA?

If, during the DPIA process, you have identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the DPC before proceeding with the project.

If the DPIA suggests that any identified risks cannot be managed and the residual risk remains high, you must consult with the Data Protection Commission before moving forward with the project.

Regardless of whether or not consultation with the DPC is required, your obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

Even if consultation is not required, the DPIA may be reviewed by the Data Protection Commission at a later date in the event of an audit or investigation arising from your use of personal data.

Should the DPIA be published?

It is not mandatory to publish a DPIA; however, there are a number of benefits to doing so. Publishing the DPIA can help to foster trust in your handling of personal data, and demonstrate accountability and transparency, particularly where members of the public are affected. This may be especially beneficial for DPIAs carried out by public bodies.

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