GIBRALTAR REGULATORY AUTHORITY

(4) Data Protection Impact Assessments

Guidance on the EU General Data Protection Regulation 2016/679 and the Data Protection Act 2004

DISCLAIMER

Please note that, on 1st January 2021, the EU General Data Protection Regulation 2016/679 ("EU GDPR") was superseded by the Gibraltar General Data Protection Regulation. The legislation however remains largely the same, and therefore, the general principles relating to the EU GDPR as may be referenced within this Guidance Note, continue to apply to the current regime.

19th May 2020

Guidance Note IR04/17 (v3)

FOREWORD

The EU General Data Protection Regulation 2016/679 (the "GDPR") came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive 95/46/EC.

Her Majesty's Government of Gibraltar amended the Data Protection Act 2004 (the "DPA") on 25th May 2018, in accordance with the introduction of the GDPR. The DPA complements the GDPR and also implements the Law Enforcement Directive 2016/680. Therefore, both pieces of legislation must be read side by side.

It is important to note that the GDPR does not generally require transposition (EU regulations have 'direct effect') and automatically became law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR and/or the DPA will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority, as the Information Commissioner, is aware of the increased obligations that the GDPR and DPA place on organisations. The Information Commissioner's aim is to alleviate some of the concerns for businesses, public-sector and third-sector organisations and assist them ensure data protection compliance.

CONTENTS

1. INTRODUCTION 1
2. WHAT IS A DPIA? 2
2.1. What does a DPIA address? 3
2.2. Joint controllers 4
3. WHEN IS A DPIA REQUIRED? 4
4. WHEN IS A DPIA NOT REQUIRED? 8
5. EXISTING PROCESSING OPERATIONS 9
6. PERFORMING A DPIA 10
6.1 At what point should a DPIA be carried out? 10
6.2 Who is obliged to carry out the DPIA? 11
6.3 What is the methodology to carry out a DPIA? 13
6.4 Publishing a DPIA 13
7. CONSULTING THE SUPERVISORY AUTHORITY 14
ANNEX A – An example of a DPIA methodology 16
ANNEX B – List of processing operations for which a DPIA is required 21
ANNEX C – List of processing operations for which a DPIA is not required 22

1. INTRODUCTION

This Guidance Note provides general advice on the requirement for organisations to carry out a Data Protection Impact Assessment ("DPIA") for any high-risk data processing activity. It is important to note that DPIAs are not a new concept, as they were a recognised procedure that organisations used to comply with data protection law under the previous regime, namely the EU Data Protection Directive 95/46/EC (the "Directive").

A DPIA is a procedure designed to assist organisations identify and minimise the privacy risks of new projects or policies. A DPIA is an important tool for accountability that will help organisations comply with the requirements under the EU General Data Protection Regulation 2016/679 (the "GDPR") and the Data Protection Act 2004 (the "DPA"), including the requirement for organisations to demonstrate that appropriate measures have been implemented to ensure compliance with data protection. Where a DPIA identifies high risks which the organisation cannot mitigate, the organisation will be obliged to consult with the Lead Supervisory Authority before engaging in the process.

It is important to note that conducting a DPIA is not mandatory for all data processing, it is only required where the intended processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1) of the GDPR)[1]. For example, this will be a requirement when a new technology is being used, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

Although undertaking a DPIA is not always compulsory, organisations may find it useful to conduct one as, if done correctly, it will help to ensure processing is GDPR compliant.

The aim of this guidance note is to provide advice on the GDPR's requirements relating to DPIAs and to assist data controllers with their role throughout this task, as they are ultimately responsible for ensuring that DPIAs are carried out according to GDPR requirements. The information provided should therefore be treated as guidance, with appropriate consideration being given to the actual legal requirements. Footnotes referencing the legislation are included so that readers are able to link and relate the guidance to the specific provisions in the law.

Acknowledgements

Where appropriate Gibraltar's Information Commissioner will seek to ensure that locally published guidance documents are consistent with others made available by fellow Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the UK's Information Commissioner's office.

[1] For processing under Part III of the DPA, a DPIA is required as stipulated in Section 73(1) of the DPA.

2. WHAT IS A DPIA?

GDPR - Article 35(7)

The assessment shall contain at least:

(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.

The GDPR does not formally define the concept of a DPIA[2], however it can be described as **a process that aims to identify and minimise the privacy risks of any given data processing activity**.

Whilst the GDPR does not define what a DPIA consists of in absolute terms, as can be seen from the requirement above, it sets out specific features that must be included in a DPIA[3] -

- a description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- 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.

[2] For processing under Part III of the DPA, see Section 73(2) of the DPA.

[3] For processing under Part III of the DPA, see Section 73(3) of the DPA, which sets out the specific features that must be included in a DPIA.

Although the above-mentioned features are mandatory, the list is non-exhaustive and flexible in that organisations may include additional features and adapt the DPIA as appropriate for the type of data used and processing intended[4].

For illustrative purposes, the Commissioner considers the following to be a useful outline of a DPIA in practice -

Step 1: *identify the need for a DPIA in relation to the envisaged processing operations and purposes (where applicable, the legitimate interest pursued by the controller);*

Step 2: *assess necessity and proportionality of the processing;*

Step 3: *identify the privacy and related risks to the rights of individuals;*

Step 4: *identify and evaluate the measures to address risks (privacy solutions);*

Step 5: *sign off and record/document the DPIA outcomes to demonstrate compliance;*

Step 6: *integrate the outcomes into the project plan.*

This DPIA process is flexible and can be integrated with an organisation's existing approach to managing projects. Importantly, it is not a static document and should be kept under review so that it may be amended in the event that any changes in circumstances require it to be adapted accordingly.

2.1. What does a DPIA address?

A DPIA may concern a single data processing operation or a set of similar processing operations that present similar high risks. In this respect, Recital 92 of the GDPR states that:

"There are circumstances under which it may be reasonable and economical for the subject of a DPIA 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."

The above means that a single DPIA may be used to assess multiple processing operations, which are similar in terms of the risks presented and the specific nature, scope, context and purposes of the processing. This may be the case where similar technology is used to collect the same sort of personal data, for the same purposes.

This is also applicable to similar processing operations implemented by various data controllers. In these cases, a reference DPIA should be shared or made publicly available, measures in the DPIA must be implemented, and a justification for conducting a single DPIA must be provided.

For example, a group of companies that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a restaurant chain (single controller) could cover video surveillance in all its restaurants with one DPIA.

[4] Organisations can develop their own DPIA framework depending on their circumstances, data included and proposed processing, as long as it contains the mandatory features.

2.2. Joint controllers

If the processing operation involves joint controllers, then each controller should define their respective obligations precisely. Their DPIA should then set out which controller is responsible for the various measures designed to manage risks and to protect the rights of the data subjects.

A DPIA may also allow controllers to assess the data protection impact of a technology product, such as hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. In this respect, it is important to note that the data controller who deploys the product will be obliged to carry out its own DPIA in respect of the implementation of that product. In certain cases, this may be informed by a DPIA prepared by the product provider.

3. WHEN IS A DPIA REQUIRED?

The GDPR does not require a DPIA to be performed for every processing operation which may result in a risk to the rights and freedoms of individuals. A DPIA should however be performed when the processing is *"likely to result in a high risk to the rights and freedoms of natural persons"* (see Article 35(1) of the GDPR)[5].

The need for a DPIA is particularly relevant when a data controller is considering introducing a new data processing technology. Article 35(3) of the GDPR[6] provides data controllers with some examples of when a DPIA is required.

GDPR - Article 35(3)

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(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;

(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; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

[5] For processing under Part III of the DPA, see Section 73(1) of the DPA.

[6] Whilst Part III of the DPA does not provide a list of examples, Section 73(4) of the DPA stipulates the information that must be considered when determining whether a type of processing is likely to result in a "high risk".

The above is meant as a non-exhaustive list. There may be processing operations that are not captured in Article 35(3) of the GDPR which may be considered "high risk" and should be subject to a DPIA. For this reason, the Article 29 Working Party [7] included in their guidelines a set of criteria that should be considered when assessing whether the processing is likely to result in a high risk.

This section aims to help data controllers identify when the processing of personal data is likely to be high-risk and require a DPIA prior to the processing.

1. Evaluation or scoring:

   This includes 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*" (Recitals 71 and 91 of the GDPR). Examples may include a financial institution that screens its customers against a credit reference database or an anti-money laundering and counter-terrorist financing or fraud database, a biotechnology company offering genetic tests directly to consumers in order to evaluate and predict the disease/health risks, an online gambling company building/using behavioural profiles to predict or alert on account activity, 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:

   This refers to 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) of the GDPR). For example, the processing may lead to the exclusion or discrimination against individuals. However, processing with little or no effect on individuals does not match this specific criterion.

3. Systematic monitoring:

   This refers to 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) of the GDPR)[8]. This type of monitoring is a criterion as personal data may be collected in circumstances where the data subject is unaware of who is collecting their personal data and how their data will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in publicly accessible spaces.

[7] The Article 29 Working Party ("WP29") was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR). The WP29 has now been replaced by the European Data Protection Board ("EDPB"). References in this document shall therefore be to the EDPB, even though the same may relate to guidance originally published by its predecessor, the WP29.

[8] The EDPB interprets "systematic" as meaning one or more of the following:
- 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 EDPB 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.

4. Sensitive data or data of a highly personal nature [9]:

   This includes special categories of data as defined in Article 9 of the GDPR (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences (see Article 10 of the GDPR)[10]. For example, this would include a general hospital keeping patients' medical records or a private investigator keeping offenders' details.
   More general types of data that might fall under this category are location data, financial data (that might be used for payment fraud) or electronic communication data. 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. Additionally, information processed by a natural person in the course of personal or household activity, such as email services, diaries, e-readers with note-taking features and various life-logging applications that may contain very personal information, would all be included in this criterion.

5. Data processed on a large scale:

   Whilst Recital 91 of the GDPR provides some guidance in relation to large scale processing operations, the GDPR does not define what constitutes "large-scale". Therefore, the Commissioner interprets this to mean a relatively significant data processing activity, taking account of the following factors -

   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; and
   d. the geographical extent of the processing activity.

6. Datasets that have been matched or combined:

   This would refer to data that may originate from two or more data processing operations performed for different purposes and/or by different data controllers, in a way that could exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects (Recital 75 of the GDPR):

   This form of data processing may require a DPIA given the increased power imbalance between the data subject and the data controller, meaning that the individual may be unable to consent to, or oppose, the processing of their data.

[9] Note, if sensitive data or data of a highly personal nature 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, may like to know what kind of food his guests are allergic to, and could process these sensitive data exceptionally without needing 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 of the GDPR).

[10] For processing under Part III of the DPA, Section 44(3) of the DPA stipulates the cases in which a "competent authority" (as defined in Section 39(1) of the DPA) may engage in sensitive personal data processing lawfully.

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 prudently oppose or consent to the processing of their data. This type of processing also poses further concern on the more vulnerable section of our population who require special protection, such as mentally ill individuals, asylum seekers, the elderly, or those who are patients. In these cases there would be an imbalance in the relationship between the position of the data subject and data controller.

8. Innovative use or applying technological or organisational solutions:

   This may include the combined use of fingerprint and facial recognition for improved physical access control, etc. The GDPR makes it clear (see Article 35(1) and Recitals 89 and 91 of the GDPR) that the use of a new technology would require a DPIA, given this can involve new forms of data collection and usage, which may result in a high risk to individuals' rights and freedoms. A DPIA would aid the data controller to understand and account for any potential personal and/or social consequences the processing might have. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy, therefore requiring a DPIA.

9. When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (Article 22 and Recital 91 of the GDPR):

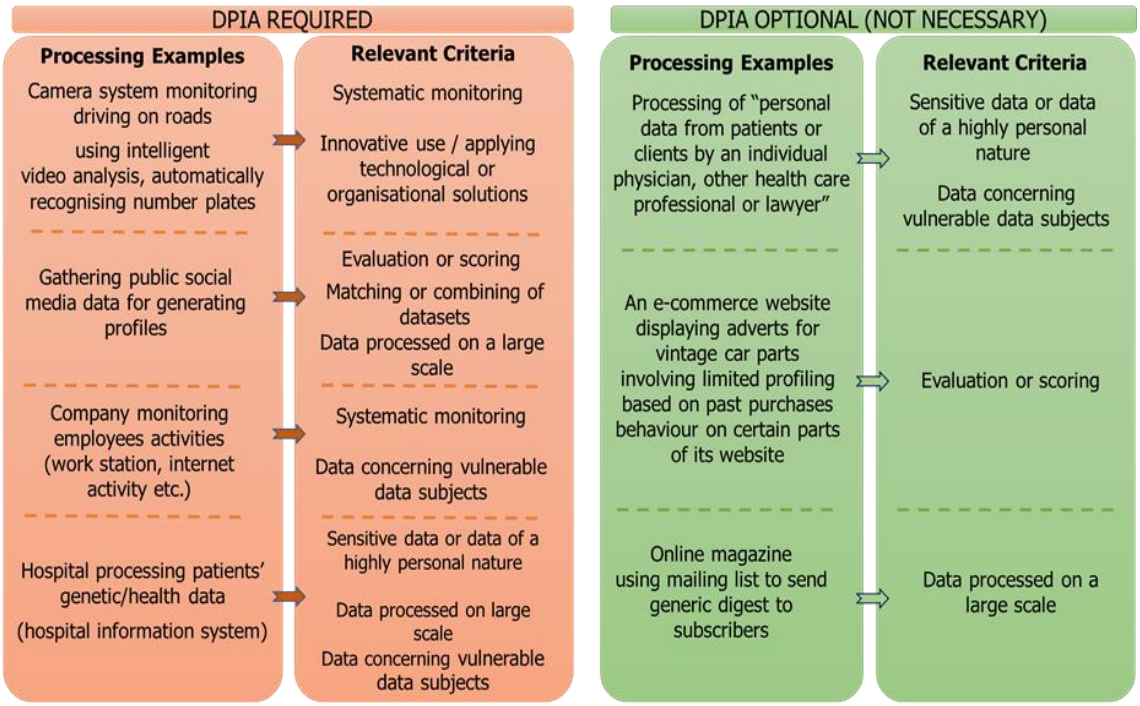
   This includes processing performed in a public area as individuals may not be able to avoid the processing, or any processing that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

The EDPB maintains that the more a processing operation meets the above criteria, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore the more likely it is to require a DPIA.

As a general rule, if a processing operation meets at least two of the above criteria, then a DPIA will be required. However, in some cases, a processing meeting only one of these criteria may require a DPIA due to the inherent high risk. Conversely, a processing operation may meet at least two criteria, but a data controller may decide that the processing is of a low risk and not carry out a DPIA. In this case, reasons would need to be thoroughly documented for not carrying out a DPIA in order to comply with the GDPR.

There might be cases where a data controller is unsure whether a DPIA is required. In these cases, the Commissioner recommends that a DPIA is still carried out as it is considered a useful tool that will help data controllers comply with data protection laws.

The following figure illustrates how specific types of data processing may or may not meet relevant criteria for a DPIA.



Notwithstanding that an organisation may determine that a processing activity does not meet the criteria that triggers the requirement to carry out a DPIA, it is important to note that under the GDPR a data controller is still required to *"maintain a record of processing activities under its responsibility".* This should include, amongst other things, the purposes of the 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) of the GDPR)[11].

In accordance with Article 35(4) of the GDPR, the Commissioner will publish a list of processing operations that are considered to require a DPIA (see ANNEX B). For the avoidance or doubt, the list will be non-exhaustive, and the absence of a data processing operation on this list should not be seen as an indication that a DPIA is not required. The list will be updated in accordance with developments.

4. WHEN IS A DPIA NOT REQUIRED?

A DPIA is not required when the processing of personal data is not *"likely to result in a high risk",* has already been authorised, or has a legal basis.

In summary, a DPIA is not required in the following circumstances:

[11] For processing under Part III of the DPA, Section 70 of the DPA contains provisions relating to records of processing activities and Section 71 of the DPA contains provisions relating to logging.

- Where the processing is *"not likely to result in a high risk to the rights and freedoms of natural persons*" (see Article 35(1) of the GDPR)[12].

- Where the processing operations have been checked by the supervisory authority before May 2018 and specific conditions have not changed.

- When the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has been carried out. In these cases, the results of a DPIA, for similar processing operations, may be used (see Article 35(1) of the GDPR).

- Where a processing operation has a legal basis in the EU or Gibraltar 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 (see Article 35(10) of the GDPR).

- Where the processing is included in a list of processing operations (established by the supervisory authority) for which no DPIA is required (see Article 35(5) of the GDPR and ANNEX C). The list may contain processing activities that comply with the conditions specified by the supervisory authority, in particular, through guidelines, specific decisions or authorizations, compliance rules, etc.

5. EXISTING PROCESSING OPERATIONS

It is important to note that under the GRPR, organisations are required to undertake a DPIA when significant changes are made to existing data processing activities (see Article 35(11) of the GDPR). For example, when a new technology has come into use or because personal data is being used for a different purpose[13]. In such cases, the processing in effect becomes a new data processing operation and therefore, could require a DPIA.

Risks can change as a result of modification 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.). In both cases new vulnerabilities may emerge. Therefore, it is important to note that the revision of a DPIA is not only beneficial for continuous improvement, but also vital to ensure an adequate level of data protection in a changing environment over a longer period of time.

Lastly, a DPIA may also become essential because the organisational or societal context for the processing activity has changed, for the reason that the effects of specific automated decisions have become more significant, new categories of natural persons become vulnerable to discrimination.

[12] For processing under Part III of the DPA, see Section 73(1) of the DPA.

[13] The EDPB means this to include terms of context, risks, purposes, personal data processed, recipients, data combinations, security measures and international transfers.

Notwithstanding the above, it is important to note that a DPIA is not required for processing operations which were checked by the supervisory authority or the data protection official, in accordance with Article 20 of the Directive, and that are performed in a way that has not changed since the prior checking.

Conversely, any data processing whose conditions of implementation have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk, should be subject to a DPIA. Further, a DPIA may be required after a change of the risks resulting from the processing operations (in terms of the context, the data collected, purposes, functionalities, recipients, data combinations, etc.). For instance, because of the use of a new technology or because personal data is being used for a different purpose.

On the other-hand, certain changes could lower the risk and a review of the risk analysis made can show that the performance of a DPIA is no longer required.

The EDPB suggest that a DPIA should be continuously carried out on existing processing activities as a matter of good practice, and be re-assessed after three years, depending on the nature of the processing and rate of change in the operation and general circumstances. Similarly, they also recommend that data processed before May 2018, which is not subject to a DPIA, should be re-assessed three years after this date or sooner, to ascertain that risks to the rights and freedoms of data subjects are still mitigated.

6.PERFORMING A DPIA

In this section advice is provided on how to conduct a DPIA, including the point at which it should be carried out, by whom, and the methodology.

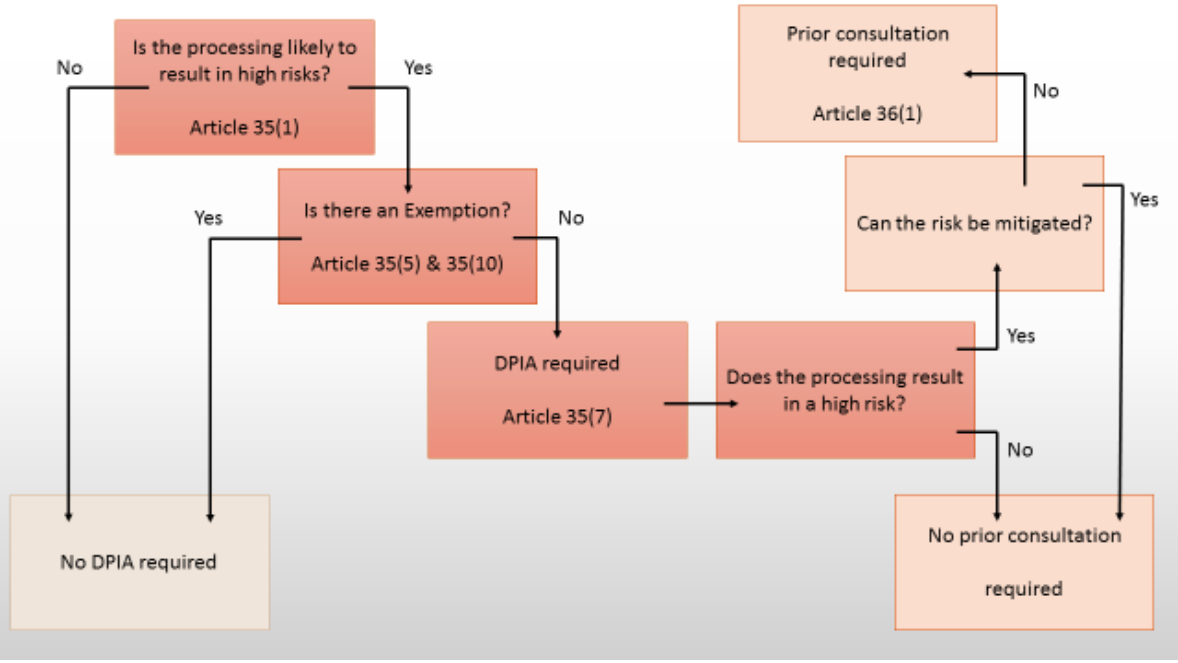
6.1 At what point should a DPIA be carried out?

GDPR – Article 35(1)

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

As outlined above and in Recital 90 of the GDPR, a DPIA should be carried out *"prior to the processing"* of personal data[14]. This is consistent with the data protection by design and by default principles (see Article 25 and Recital 78 of the GDPR)[15].

The following diagram illustrates the basic principles relating to DPIAs under the GDPR:



A DPIA should be carried out as early as practicable in the design of the processing operation, even if some of the processing operations are unknown. As a DPIA is updated throughout its development, it will ensure that data protection and privacy are considered, and it will allow the controller to develop solutions that ensure compliance.

Data controllers should be prepared to repeat individual steps of the assessment as the development process progresses, particularly when a processing operation is dynamic and is subject to continuous change.

6.2 Who is obliged to carry out the DPIA?

Under the GDPR, the data controller is responsible for ensuring that a DPIA is carried out (Article 35(2) of the GDPR). Whilst a DPIA may be conducted by someone else, inside or outside the organisation, the data controller remains accountable for that task.

[14] For processing under Part III of the DPA, see Section 73(1) of the DPA, which stipulates that a DPIA should be conducted "*prior to the processing*".

[15] For processing under Part III of the DPA, see Section 66 of the DPA.

The data controller must seek advice from the Data Protection Officer (DPO)[16] where designated (Article 35(2) of the GDPR) and this consultation, including any decisions taken, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c) of the GDPR)[17].

Where the processing is wholly or partly performed by a data processor, the processor should assist the controller in conducting the DPIA, taking into account the nature of the processing and the information available to the processor (Article 28(3)(f) of the GDPR).

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

- these views can be acquired through a variety of means, depending on the context (for example, studies related to the purpose and means of the processing, 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; and
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.

It is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules. For example -

- business departments proposing to carry out a DPIA should provide input and be involved in the validation process of the DPIA;
- where appropriate, professionals should be consulted (lawyers, technicians, security experts, sociologists, ethics professionals, etc.);
- the roles and responsibilities of the processors must be contractually defined;
- if the Chief Information Security Officer ("CISO"), if appointed, or the DPO suggests that the data controller carries out a DPIA on a specific processing operation, they should help the stakeholders with the methodology, assist in the evaluation of the risk assessment and whether the residual risk is acceptable, and contribute to the development of knowledge specific to the data controller context; and
- the CISO, if appointed, and/or the IT department, should provide assistance to the data controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

[16] See the Information Commissioner's Guidance Note IR03/17 (3) Data Protection Officer (www.gra.gi/data-protection/guidance). For processing under Part III of the DPA, see Sections 78-80 of the DPA, relating to the requirements for the designation, position and tasks of a DPO.

[17] For processing under Part III of the DPA, see Section 80(1)(b) of the DPA, which stipulates the tasks the DPO must undertake in regard to the DPIA. In this respect, the DPO must provide advice on the carrying out of the DPIA and monitor compliance with Section 73 of the DPA.

6.3 What is the methodology to carry out a DPIA?

As described earlier in Section 2, there are certain requirements that must be included in a DPIA. Beyond this, a data controller may adapt or develop a DPIA in a manner that is appropriate to the processing activity or activities it undertakes.

There are a number of established methodologies within the EU and worldwide which take account of the components of a DPIA as described in the GDPR. The development of sector specific DPIA frameworks is also encouraged, as the inclusion of sectoral knowledge may allow DPIAs to address the specifics of a particular type of processing operation (for example, particular types of data, corporate assets, potential impacts, threats, measures etc.).

It is up to the data controller to choose a methodology, however, regardless of its form, a DPIA must be a genuine assessment of risks, allowing data controllers to take measures to address them. Further, where necessary, the data controller should carry out a review to assess if the processing is performed in accordance with the DPIA at least when there is a change of risk represented by the processing operation (see Article 35(11) of the GDPR).

To assist data controllers, the Commissioner provides an example of a DPIA methodology in ANNEX A.

6.4 Publishing a DPIA

Publishing a DPIA is not mandatory under the GDPR. However, data controllers should consider publishing their DPIA, part of their DPIA, or even a summary of their DPIA, for various reasons.

Publishing a DPIA may help foster trust in the data 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 simply consist of a summary of the DPIA' s main findings, or even a statement that a DPIA has been carried out.

However, when high residual risks cannot be mitigated, the Commissioner is to be consulted[18] and the DPIA must be provided (Article 36(3)(e) of the GDPR)[19]. The Commissioner may provide his advice and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable on public access to official documents.

[18] See Article 36(1), Recital 84 and Recital 92 of the GDPR. Note that for processing under Part III of the DPA, where, under Section 74(1) of the DPA, a controller intends to create a filing system, prior consultation in the context of DPIAs is required as prescribed by Section 74(2) of the DPA.

[19] For processing under Part III of the DPA, see Section 74(3)(a) of the DPA.

7. CONSULTING THE SUPERVISORY AUTHORITY

GDPR - Article 36 (1)

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

As outlined above, the Commissioner must be consulted if residual risks are high and data controllers are unable to appropriately mitigate risks when conducting a DPIA[20].

For example, the processing of medical data on a large scale is likely to result in a high risk, and therefore likely to require a DPIA. In such cases, it is the obligation of the data controller to evaluate the risks to the rights and freedoms of data subjects and to identify the measures[21] envisaged to reduce those risks to an adequate level, and to demonstrate compliance with the GDPR (Article 35(7)of the GDPR)[22].

Measures could include appropriate technical and organisational security procedures (for example, effective full disk encryption, robust key management, appropriate access control, secured backups, etc.) on laptops storing personal data, along with existing policies (such as notice, consent, right of access, right to object, etc.). This example demonstrates how risks can be managed by data controllers and how such processing can proceed without consulting the Commissioner where all identified risks have been sufficiently addressed.

In cases where the residual risks remain high and cannot be adequately mitigated, such as instances where the data subjects may encounter significant or even irreversible consequences which they may not overcome (for example, unauthorised access to data leading to a threat on the life of data subjects), and/or when it seems obvious that the risk will occur (for example, where a data controller cannot reduce the number of individuals accessing the data because of its sharing), the data controller must consult the Commissioner (see Recital 84 of the GDPR).

Further, the controller will have to consult and/or obtain prior authorisation from the Commissioner whenever Gibraltar law requires a data controller to do so in relation to processing for the performance of a task carried out by the data controller in the public

[20] See Article 36(1), Recital 84 and Recital 92 of the GDPR. Note that for processing under Part III of the DPA, where, under Section 74(1) of the DPA, a controller intends to create a filing system, prior consultation in the context of DPIAs is required as prescribed by Section 74(2) of the DPA.

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

[22] For processing under Part III of the DPA, see Section 73(3)(c) and (d) of the DPA.

interest, including processing in relation to social protection and public health (Article 36(5) of the GDPR).

Regardless of whether consultation is required, based on the level of residual risk, an organisation will still need to meet their obligations of retaining a record of the DPIA and must update the DPIA as and when necessary.

ANNEX A – An example of a DPIA methodology

Step 1: Identify the need for a DPIA in relation to the envisaged processing operations and purposes (where applicable, the legitimate interest pursued by the controller).

1. Describe and record legitimate reasons for undertaking the project, the overall aims and intended outcomes.[23]
    - This should include a functional description of the processing operation, taking into account the nature, scope, context and purposes of the processing (Recital 90 of the GDPR)[24].

2. Develop and answer a set of screening questions to identify a proposal's potential impact on privacy.
    - This should clarify and record what personal data is going to be used, who the recipients of the data will be and the period for which the personal data will be stored.
    - Organisations should also identify the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels).

3. Consider how the project management activity can address privacy issues.
    - Organisations should take into account compliance with approved codes of conduct (Article 35(8) of the GDPR).
    - Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR)[25], should be taken into account as well.

4. Begin to discuss privacy issues with stakeholders and involve interested parties.
    - Seek advice of the DPO (Article 35(2) of the GDPR)[26].
    - Seek assistance and information from the processor as required in Article 28(3)(f) of the GDPR[27].
    - Seek the views of data subjects or their representatives (Article 35(9) of the GDPR).

5. Adapt the project development process to address privacy concerns.

The above is a generic approach, the level of detail can be decided by the organisation and will depend on various factors, including the time and resources available to the project team, although this should not impact the effectiveness of the DPIA or the controller's ability to comply with GDPR and/or DPA requirements.

---

[23] For processing under Part III of the DPA, see Section 74(2) and 73(3)(a) of the DPA.

[24] For processing under Part III of the DPA, see Section 73(4) of the DPA.

[25] For processing under Part III of the DPA, see Chapter 5 of Part III of the DPA regarding transfers of personal data to third countries.

[26] For processing under Part III of the DPA, see Section 80(1)(b) of the DPA.

[27] For processing under Part III of the DPA, see the obligations of data processors as stipulated in Section 69 of the DPA and specific obligations with respect to security at Section 75 of the DPA.

Another important aspect of a DPIA is describing information flows in a project. This process can help organisations identify unforeseen or unintended uses of data, for example data sharing.

To describe information flows, organisations should explain and document how information will be processed. Information flows may be integrated into similar exercises already completed or envisaged, such as information audits, information maps, user journeys or information asset registers. Project proposals or similar documents that may have been produced to determine how personal data might be processed within a project, are also useful for this activity.

Information flows may be recorded in a format that meets the needs of the organisation. This should then be used as part of the final DPIA report.

If the data controller decides that a DPIA is not to be carried out, it is recommended that a record of this first step is nevertheless kept.

Step 2: Assess necessity and proportionality of processing.

In order to complete this step, organisations must assess and document the necessity and proportionality of the project in relation to the purposes for conducting the project (Article 35 (7)(b) of the GDPR)[28].

To comply with GDPR requirements, organisations should -

- determine the extent to which a project collects and processes personal data for specified, explicit and legitimate purposes, as noted in Article 5(1)(b) of the GDPR;
- ensure that the personal data processed is adequate, relevant and limited to what is necessary, as specified in Article 5(1)(c) of the GDPR;
- establish a policy for the project that guarantees limited storage duration of personal data, as noted in Article 5(1)(e) of the GDPR; and
- ensure the lawfulness of processing as outlined in Article 6 of the GDPR[29].

Meeting the above requirements will help organisations evaluate whether the impact on privacy is proportionate to the outcomes to be achieved by a particular project.

Step 3: Identify the privacy and related risks to the rights of individuals.[30]

At this stage, organisations should assess the potential privacy issues associated with a project. Risks to individuals can be categorised in different ways and it is important that all types of risks are considered. These can range from risks of physical safety, material impacts (such as financial loss) or moral impacts (such as distress caused).

[28] For processing under Part III of the DPA, note that Section 73 of the DPA does not explicitly state that the necessity and proportionality of the processing must be recorded as part of the DPIA. However, an assessment of these aspects of the processing would nevertheless assist in demonstrating compliance with Section 73(3)(b) and 73(3)(d) of the DPA.

[29] For processing under Part III of the DPA, see the requirements in regard to the principles of processing in Chapter 2 of Part III of the DPA.

[30] See Article 35(7)(c) of the DPA. For processing under Part III of the DPA, see Section 73(3)(b) of the DPA.

This step does not require organisations to decide on a particular method to carry out a DPIA. Organisations may implement their existing project management or risk management methodologies to help them identify risks and adjust them as appropriate.

However, the DPIA process must specifically include an evaluation of risks posed to the rights of data subjects[31] as listed below -

- the right to be informed (Articles 12, 13 and 14 of the GDPR);
- the right of access (Article 15 of the GDPR);
- the right to rectification (Article 16 of the GDPR);
- the right to erasure (Article 17 of the GDPR);
- the right to restrict processing (Article 18 of the GDPR);
- the right to data portability (Article 20 of the GDPR);
- the right to object (Article 21 of the GDPR); and
- rights in relation to automated decision making and profiling (Article 22 of the GDPR).

Additionally, as well as considering and complying with the GDPR Articles more generally, organisations must also pay particular attention to the GDPR requirements which relate to the following -

- data processor(s) (Article 28 of the GDPR)[32]; and
- prior consultation (Article 36 of the GDPR)[33].

It is essential that all of the identified privacy risks are recorded at this stage. It may also be useful to use a privacy risk register to describe the risks in terms of origin, nature, particularity, likelihood and severity (Recital 90 of the GDPR). Small scale projects may have a less formal approach to risk, and this can also be reflected in the privacy risk register.

Step 4: Identify and evaluate the measures to address risks (privacy solutions).[34]

Organisations need to identify possible privacy solutions to address the risks that have been identified in the above steps.

A DPIA should set out the organisation's options for addressing each risk that has been identified and state whether each option would result in the risk being -

- eliminated;
- reduced; or
- accepted.

[31] For processing under Part III of the DPA, see the requirements in regard to the rights of data subjects in Chapter 3 of Part III of the DPA.

[32] For processing under Part III of the DPA, see the obligations of data processors as stipulated in Section 69 of the DPA and specific obligations with respect to security at Section 75 of the DPA.

[33] Note that for processing under Part III of the DPA, where, under Section 74(1) of the DPA, a controller intends to create a filing system, prior consultation in the context of DPIAs is required as prescribed by Section 74(2) of the DPA.

[34] See Article 35(7)(d) of the DPA. For processing under Part III of the DPA, see Section 73(3)(c) and (d) of the DPA.

It is important to remember that the aim of a DPIA is not to completely eliminate any impact a project may have on privacy. The purpose of the DPIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented.

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. The costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include -

- deciding not to collect or store particular types of information;
- devising retention periods which only keep information for as long as necessary and planning secure destruction of information;
- implementing appropriate technological security measures;
- ensuring that staff are properly trained and are aware of potential privacy risks;
- developing ways to safely anonymise the information when it is possible to do so;
- producing guidance for staff on how to use new systems and how to share data if appropriate;
- using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests;
- taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary;
- selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf; and/or
- producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Privacy risks and solutions should be recorded on a privacy risk register, as mentioned in the previous step. The privacy risk register should be updated to reflect how these measures have changed the level of risk. When an organisation accepts risks, it should explain why it has decided to do so. The register should record each risk, explain what action has been taken or will be taken and identify who is responsible for approving and implementing the solution.

Step 5: Sign off and record/document the DPIA outcomes to demonstrate compliance.

This step emphasises the importance of keeping a record of the DPIA as this will ensure the necessary measures are implemented to appropriately identify and reduce privacy risks. It can also be used to assure the public and other stake holders that the project has been thoroughly assessed.

The report should include the following -

- an overview of the project, explaining why it was undertaken and how it will impact on privacy;
- material or references to the material produced throughout the previous DPIA steps, for example the description of data flows and the privacy risk register; and
- a description of how the privacy risks were identified and how they will be addressed.

A DPIA does not necessarily require a formal signing-off process but this will depend on the nature of the project. If an organisation is working on large-scale project with a higher level of risk, it would be good practice to ensure that the DPIA has been approved at a senior level. For smaller projects, it can be appropriate for the project leader to accept the privacy risks. A signing-off can also help to ensure that the necessary actions are followed up.

Important: The Commissioner does not take a role in approving or signing-off DPIAs. This process has been developed to focus on self-assessment, and every DPIA relies on an organisation's understanding of its own practices.

Step 6: Integrate the outcomes into the project plan.

The results of the DPIA should be fed back into the wider project management process. This will usually need to take place while the project is still being developed.

Organisations should take care to ensure that the steps taken as a result of the DPIA have been properly implemented and are having the desired effect.

If a project develops or changes during its lifecycle, the organisation may need to revisit the screening questions to ensure the DPIA is still appropriate. This might be especially important with particular project management methodologies which may not have a fixed set of requirements at the outset.

As with other aspects of the DPIA, a review of the privacy outcomes can be built into existing procedures. If an organisation were to review the general implementation of a new project after a certain period, it should be possible to include a process for checking the work arising from the DPIA as well. DPIAs should be developed with the aim to integrate them into an organisation's own project management processes and most project management methodologies include a post project review.

ANNEX B – List of processing operations for which a DPIA is required

As detailed above in Section 3, below is a list of processing operations that are considered to require a DPIA. This list is based on guidelines adopted by the EDPB on DPIAs (WP248rev01). Our list therefore complements and further specifies these guidelines. The list will be updated in accordance with developments.

1. **Innovative technology**: Processing involving the use of innovative technologies, or the novel application of current technologies (including AI). A DPIA is mandatory for this type of processing when combined with any of the criteria within the European guidelines.
2. **Denial of service**: Data processing that affects an individual's access to a product, service, opportunity or benefit, due to automated decision-making, profiling or involves the processing of special category data.
3. **Large-scale profiling:** A DPIA is required for any large-scale profiling of individuals.
4. **Biometrics:** A DPIA is compulsory for any processing of biometric data when it is combined with any of the criteria from the European guidelines.
5. **Genetic data:** Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
6. **Data matching:** Processing that involves the combination, comparison or matching of personal data attained from more than one source.
7. **Invisible processing:** When personal data is processed without being directly obtained from the data subject due to an impossible or disproportionate effort to comply with Article 14 of the GDPR. A DPIA is mandatory for this type of processing when combined with any of the criteria within the European guidelines.
8. **Tracking:** Data processing involving the tracking of an individual's location or behaviour, including online activity. A DPIA is mandatory for this type of processing when combined with any of the criteria within the European guidelines.
9. **Targeting of children or other vulnerable individuals:** A DPIA is mandatory for the processing of the personal data of children or other vulnerable groups for the purpose of marketing, profiling, automated decision-making or for offering online services directly to children.
10. **Risk of physical harm:** A DPIA is obligatory due to a breach of this type of data processing that could cause a physical, health or safety risk to individuals.

ANNEX C – List of processing operations for which a DPIA is not required

IMPORTANT NOTE

This document is purely for guidance and aims to supplement the EDPB's Guidelines on Data Protection Impact Assessments[35]. The document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR will apply directly to them. The responsibility to become familiar with the GDPR and comply with its provisions therefore lies with the organisation.

Where necessary, the Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR, the GDPR will take precedence.

[35] Originally published by the WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (4 October 2017).

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi