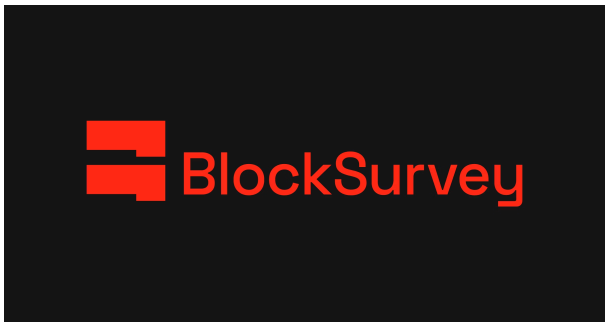

BlockSurvey	DPIA Guidance Note
Version – 3.0	**Release Date – 11-04-2026**

Version Control

Version Number	Date of Release	Nature / Description of Change	Prepared / Changed By	Approved By
1.0	22-02-2024	Initial	Priya	Wilson Bright J
2.0	11-04-2025	Annual Review	Priya	Wilson Bright J
3.0	11-04-2026	Annual Review	Priya	Wilson Bright J

1) Introduction

Article 35 of the GDPR provides for the conduct of a Data Protection Impact Assessment (DPIA). Data Protection Impact Assessments are a tool designed to enable organisations to work out the risks that are inherent in proposed data processing activities before those activities commence. This enables organisations to address and mitigate those risks before the processing begins.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. A DPIA is a process for building and demonstrating compliance.

2) Iterative Process of DPIA

2.1 Description of envisaged processing.

2.2 Assessment of necessity and proportionality.

2.3 Measures already envisaged.

2.4 Assessment of risks to the rights and freedoms.

2.5 Measures envisaged to address the risks.

2.6 Documentation.

2.7 Monitoring and Review.

3)How to Conduct a DPIA

3.1 The DPIA should be carried out “prior to the processing”.

3.2 The carrying out of a DPIA is only mandatory where processing is “likely to result in a high risk to the rights and freedoms of natural persons.”

3.3 It is particularly relevant when a new data processing technology is being introduced.

3.4 When there is 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, which result in legal effects or similarly significant effects, with respect to the natural persons.

3.5 When there is processing of special categories of personal data under Article 9(1) of the GDPR.

3.6 When there is systematic monitoring of personal data in a publicly accessible area on a large scale

3.7 The DPIA should be conducted when the processing does not meet the exceptions laid down under Article 35(5) and (10).

3.8 The controller is responsible for ensuring that the DPIA is carried out.

3.9 The controller must also seek the advice of the Data Protection Officer (DPO).

3.10 If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.

3.11 Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e., the residual risks are still high), consultation with the supervisory authority is required.

4) Criteria to be followed while conducting a DPIA

4.1 Evaluation or scoring

4.1.1 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”.

4.2 Automated decision making with legal or similar significant effect

4.2.1 This includes processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person”. For example, the processing may lead to the exclusion or discrimination against individuals.

4.3 Systematic monitoring

4.3.1 This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

4.4 Sensitive data or data of a highly personal nature

4.4.1 This includes special categories of personal data as well as personal data relating to criminal convictions or offences.

4.4.2 These personal data are considered as sensitive because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud).

4.4.3 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.

4.4.4 This may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.

4.5 Data processed on a large scale

4.5.1 When determining whether the processing is carried out on a large scale, following factors should be considered:

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

- the geographical extent of the processing activity.

4.6 Matching or combining datasets

4.6.1 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.

4.7 Data concerning vulnerable data subjects

4.7.1 Vulnerable data subjects may include children, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

4.8 Innovative use or applying new technological or organisational solutions

4.8.1 The GDPR makes it clear that the use of a new technology mandates carrying out a DPIA.

4.8.2 This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms.

4.8.3 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.

4.8.4 Examples of new technological or organisational solutions are - combining use of fingerprint and face recognition for improved physical access control, etc.

4.9 When the processing in itself "prevents data subjects from exercising a right or using a service or a contract"

4.9.1 This includes processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

5. How to fill a DPIA?

5.1 Identify the need for a DPIA

5.1.1 Explain broadly what project aims to achieve and what type of processing it involves.

5.1.2 Refer or link to other documents, such as a project proposal.

5.1.3 Summarise the identification of the need for a DPIA.

5.2 Describe the processing

5.2.1 Describe the nature of the processing:

- How will you collect, use, store and delete data?

- What is the source of the data?

- Will you be sharing data with anyone?

- What types of processing identified as likely high risk are involved?

- Refer to a flow diagram or other way of describing data flows.

5.3 Describe the scope of the processing

- What is the nature of the data, and does it include special category or criminal offence data?

- How much data will you be collecting and using and how often?

- How long will you keep it?

- How many individuals are affected?

- What geographical area does it cover?

5.4 Describe the context of the processing

- What is the nature of your relationship with the individuals?

- How much control will they have?

- Would they expect you to use their data in this way?

- Do they include children or other vulnerable groups?

- Are there prior concerns over this type of processing or security flaws?

- What is the current state of technology in this area?

- Are there any current issues of public concern that you should factor in?

- Are you signed up to any approved code of conduct or certification scheme?

5.5 Describe the purposes of the processing

- What do you want to achieve?

- What is the intended effect on individuals?

5.6 Consider how to consult with relevant stakeholders

5.6.1 Describe when and how you will seek individuals' views.

- Who else do you need to involve within your organisation?

- Do you need to ask your processors to assist?

- Do you plan to consult information security experts, or any other experts?

5.7 Describe compliance and proportionality measures

- What is your lawful basis for processing?

- Does the processing actually achieve your purpose?

- Is there another way to achieve the same outcome?

- How will you prevent function creep?

- How will you ensure data quality and data minimisation?

- What information will you give individuals?

- How will you help to support their rights?

- What measures do you take to ensure processors comply?

- How do you safeguard any international transfers?

5.8 Risk Identification

5.8.1 Describe source of risk and nature of potential impact on individuals.

5.8.2 Include associated compliance and corporate risks as necessary.

5.8.3 Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk

5.9 Sign off & record outcomes

5.9.1 Integrate actions back into project plan, with date and responsibility for completion

5.9.1 The DPO should also review ongoing compliance with DPIA