Langslide

DPIA Guidance Note

Version 1.0

PURPOSE

The purpose of a DPIA is to describe data processing activities, assess their necessity and proportionality, and manage the risks to individuals' rights. DPIAs help evaluate measurements, thereby serving as necessary accountability tools for demonstrating that appropriate compliance measures are in place.

SCOPE

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 evaluating them and evaluating the measures to address them.

DPIAs are essential tools as they help controllers demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. A DPIA is a process for building and demonstrating compliance.

This methodology supports the Data Protection Impact Assessment (DPIA) in all business departments of Rudramsa Systems Pvt. Ltd. (herein referred to as the Organization).

DEFINITION

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

- **DPO:** Data Protection officer
- **PII:** Personally Identifiable Information
- **Controller:** The controller is an entity or person that determines the purposes
- **Processor:** The processor is an entity or person that processes personal data on behalf of the controller
- **Personal data:** Any information about an identified or identifiable natural person ("data subject"). An identifiable person is a natural person who can be identified, directly or indirectly, by reference to such information as name, ID card number, location, and other identifiable information, or one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity, and other relevant information. Personal data includes a natural person's email address, telephone number, biometric features (such as fingerprint), location, IP address, health information, religious belief, social security number, and marital status.
- **Sensitive personal data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data or biometric data to uniquely identify a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.
- **Business contact information:** This means an individual's name, position name or title, business telephone number, business address, business electronic mail address, business fax number, and any other similar information about the individual not provided by the individual solely for his purposes.
- **Data Protection Impact Assessment (DPIA):** A process designed to describe the processing activities, assess the necessity and proportionality of processing, and p manage the risks to the rights and freedoms of natural persons resulting from the cessing of personal data.
- **Processing/Processing activity:** Means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

ROLES AND RESPONSIBILITIES

- The DPO should also review ongoing compliance with DPIA.
- The Privacy Officer ensures appropriate security measures are taken to protect Personal Data.
- DPIA is mandatory for data controllers. Where significant parts of the processing occur with the processor, the processor must assist with the DPIA at the controller's request.
- DPIA must be done before processing personal data.
- The Data Protection Officer oversees the overall data protection impact assessment process.
- The Data Protection Officer must decide whether the data subjects will be consulted when performing the DPIA.
- The DPIA Register must be used when performing the Data Protection Impact Assessment. It collects the data, assesses the risks, defines mitigation measures, and reports the DPIA results.
- Where there is a joint-controller relationship, each controller must carefully define which part of the data processing activities belongs to whom.

DPIA METHODOLOGY

Steps in the DPIA

Step 1: Listing and grouping data processing activities

- The Data Protection Officer must review all the activities in the Inventory of Processing Activities, consider any new activities not yet listed in the Inventory, and list all the data processing activities in the DPIA Register.
- A single assessment can be done simultaneously if several data processing activities present similar high risks. The Data Protection Officer decides which activities will be assessed together.

Step 2: Answering the threshold questionnaire

- The Data Protection Officer must answer all the Threshold questions for each data processing activity with the help of the responsible persons for each activity.
- These Threshold questions are necessary to determine whether a processing activity is likely to result in a high risk to the rights and freedoms of natural persons.

Step 3: Determine whether a complete data protection impact assessment is needed

- The Data Protection Officer will determine whether a data processing activity needs to undergo a DPIA from the Threshold questionnaire. If any of the questions from the Threshold questionnaire are answered with "Yes," a DPIA needs to be conducted for that particular data processing activity.
- Even if the answer to all the questions in the Threshold questionnaire is "No," the Data Protection Officer can decide to perform the DPIA if the company needs a clearer view of the risks involved.

Step 4: Answer the Data Protection Impact Assessment Questionnaire

- For each data processing activity where the DPIA is required, the Data Protection Officer completes the DPIA Questionnaire in the DPIA Register. All mandatory elements must be completed.
- The purpose of these questions is to get a systematic description of the processing activities.

Step 5: Identify and list key security risks

- Once the Data Protection Officer has completed the Data Protection Impact Assessment Questionnaire, they must use the findings to identify and list key security risks associated with the processing activity.
- In particular, the Data Protection Officer must consider the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

Step 6: Determine how to mitigate the risks

- Once the key risks are identified and listed, the Data Protection Officer should formulate a mitigation plan and insert it in the questionnaire. The following information needs to be specified:
- Safeguards that need to be implemented
- Responsibilities for the implementation
- Deadlines for the implementation

Step 7: Record the implementation

- Once a safeguard is implemented, the Data Protection Officer must record it in the DPIA Questionnaire under the "Record of Completion" column.

Consultations with the Supervisory Authority

- Suppose the DPIA results indicate that data processing activity would result in a high risk even if the security measures are implemented. In that case, the Data Protection Officer must consult the supervisory authority before the data processing occurs.
- In this case, the Data Protection Officer must provide the following information to the supervisory authority:
    - Responsibilities of the controller, joint-controller(s) and processor(s)
    - Purpose and means that will be used for processing
    - Security measures intended to protect the data
    - Contact details of the Data Protection Officer and
    - Results of the DPIA

Regular review of the DPIA

The Data Protection Officer must review the DPIA in any of the following cases:

- If risks related to data processing activities change or
- If there is a significant change in the data processing activities or
- If there is a change in the legal requirements,
- If a company acts as a processor, and the controller asks for a reviewed DPIA

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya