ISSN: 2755-0214

Journal of Economics & Management Research

SCIENTIFIC Research and Community

Review Article

Open Access

Assessing for Assurance: The Critical Role of DPIAs in Data Privacy Compliance

Puneet Matai

Associate Director – Enterprise Data Governance Group Santander Bank N.A., USA

Executive Summary

This article discusses the critical role of Data Protection Impact Assessments (DPIAs) in data privacy compliance, focusing on their importance, process, and implementation strategies. It highlights DPIAs as essential tools for organizations to safeguard personal data, comply with global privacy laws like GDPR, and build trust with stakeholders. Embracing DPIAs proactively enhances data management, mitigates risks, ensures legal compliance, and improves operational efficiency, making them crucial in today's data-driven world.

***Corresponding author**

Puneet Matai, Associate Director – Enterprise Data Governance Group Santander Bank N.A., USA

Received: January 10, 2022; **Accepted:** January 17, 2022; **Published:** January 30, 2022

Keywords: DPIA, Data Protection Impact Assessment, GDPR Compliance, Privacy Risks, Personal Data, Global Privacy Laws

Introduction

Data Protection Impact Assessments (DPIAs) are essential in safeguarding personal data and ensuring compliance with global privacy laws. In today's data-driven world, understanding DPIAs becomes essential for organizations aiming to prioritize privacy considerations and mitigate risks associated with data processing activities.

According to GDPR, the responsibility of conducting DPIA falls on the data controller, who is the entity or organization responsible for determining the purposes and methods of processing personal data according to GDPR.

This article aims to demystify DPIAs to highlight their importance, process, and implementation strategies. It will also provide an overview to help organizations assess the knowledge and tools necessary to explore the complexities of data privacy compliance effectively.

Understanding DPIAs

What is DPIA?

According to the Data Protection Commission [1], a Data Protection Impact Assessment (DPIA) is a structured procedure which aims at recognizing risks that may emerge from handling personal data and reducing these risks as much and as early as feasible.

European Data Protection Supervisor [2] defines DPIA as the process designed to offer confidence in managing the privacy and data protection risks associated with 'risky' processing activities.

What is the role of a DPIA?

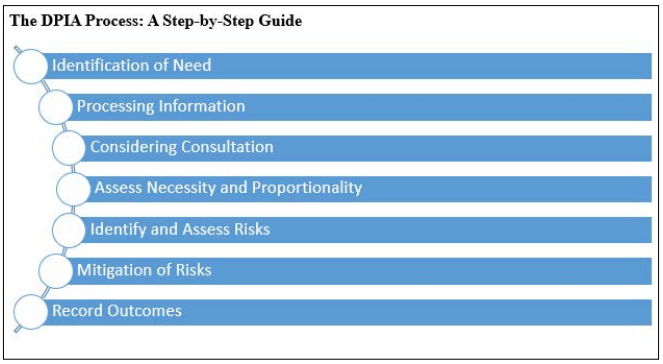
To make you understand in simple terms, the role of DPIA is as a safety check for personal data. It's like making sure your house has sturdy locks and alarms to protect your belongings. Here's how it works:

- DPIA is needed when personal data could pose a high risk to people's privacy. For example, if the bank checks a customer's credit history.
- DPIA looks at how much risk there is present to people's privacy and figures out ways to lower that risk.
- National Data Protection Authorities and the European Data Protection Board can ensure when DPIA is needed.
- DPIA is not a one-time process, but it's a tool which keeps checking and improving the safety of personal data.

Legal and Ethical Backdrop Necessitating DPIAs in Global Organizations

DPIAs are mandated by legal frameworks and ethical considerations within global organizations. Laws such as the General Data Protection Regulation (GDPR) in the EU require organizations to conduct DPIAs for processing activities. DPIAs align with the fundamental right to privacy. They ensure that organizations prioritize privacy considerations and implement necessary safeguards when handling personal data.

DPIAs also serve as a risk management tool which identifies individual rights. Beyond legal requirements, conducting DPIAs reflects an organization's ethical responsibility towards data subjects. Overall, it demonstrates commitment, builds reputation, and enhances trust towards an organization.



Step 1: Identification of Need

The identification of the need for DPIA can be like planning to build a new house. Before you start, you should check if the land is suitable [3]. Similarly, in data processing, DPIAs are used to check what might cause big privacy risks like collecting sensitive information on a large scale.

Step 2: Processing Information

The process would be like drawing a blueprint for your house. DPIAs are implemented by describing the type of data being used, collected, or assessed in future.

Step 3: Considering Consultation

Consultation is conducted when an organisation is uncertain about implementing DPIAs. If the processing of data affects people like existing customers, you ask for the consultant's views.

Step 4: Assess Necessity and Proportionality

The next step is to collect the necessary data for your purpose, not more. Article 29 guidelines on data protection suggest the inclusion of a lawful basis for processing, implementation of individual rights, safeguarding for international data transfers etc.

Step 5: Identify and Assess Risks

Risk assessment is a critical component as it helps in evaluating freedom by considering the factors of data security vulnerabilities, potential harm, and the likelihood of adverse impacts.

Step 6: Identify Measures to Mitigate Risks

Once risks are identified, measures to mitigate these risks are developed and implemented. Measures may include data encryption, access controls, and regular audits to ensure compliance.

Step7: Sign off and Record Outcomes

Finally, the outcome of the DPIA is documented. This documentation includes the decisions made and actions taken to safeguard data protection and privacy.

Why DPIAs are Essential

Importance of DPIAs in Preempting Data Privacy Risks and Compliance with Global Privacy Laws

DPIAs are essential for several reasons which contribute to an organization's data protection strategy and compliance with global privacy laws:

- DPIAs ensure compliance with global privacy laws such as GDPR. It is mandated by GDPR whenever initiating a new project with a potential "high risk" to personal data. Non-compliance with GDPR can lead to penalties, including fines of up to $20 million or 4% of annual revenue, whichever is greater [4].
- DPIs are important because they promote data minimization and quality by assessing the necessity and proportionality of data collected. DPIAs also assess the compliance of third-party data processors which ensures contractual arrangements, security measures, and data handling practices meet data protection standards.
- The evaluation of safeguards for international data transfers is also ensured through compliance with regulations governing the cross-border transfer of personal data. This includes assessing the adequacy of transfer mechanisms such as standard contractual clauses and other legal instruments.

Implementing DPIAs in Your Organization

How to Integrate the DPIA Process into Organizational Workflows?

Assign Responsibility

Designate a DPIA coordinator or Data Protection Officer (DPO) to oversee the DPIA process.

Create a DPIA Checklist

Develop a checklist outlining the steps and criteria for when a DPIA is required, such as while processing sensitive data or using new technologies.

Include DPIA in Project Planning

Integrate DPIA as a standard step in the project planning process. Ensure that DPIAs are conducted before starting new data processing activities.

Review and Update Regularly

Periodically review and update DPIAs, especially when there are changes in processing activities, technologies, or risks.

Document and Communicate

Thoroughly document DPIA findings, assessments, and risk mitigation measures. Communicate the actions to relevant stakeholders for transparency and compliance.

Roles, Responsibilities, and Involvement in the DPIA Process

The roles and responsibilities of the following designation are important in the DPIA process whose involvement can ensure seamless implementation [5]:

Researcher

- Demonstrates implementation of DPIA measures.
- Participates in the DPIA process
- Contact the P&S coordinator for changes related to DPIA measures.

Ethics Board

- Determines if DPIA is necessary.
- Provides advisory role and discipline-specific guidance.
- Represents data subject's interests and advises the dean on ethics and privacy.

Data Subject

- Provides input on processing aspects like commercial interests and security measures.

P&S Coordinator

- Coordinates the DPIA process.
- Represents the dean on Privacy and Security policies.
- Ensures measures are implemented and documented.

DCC Consultant

- Advice on technical measures.
- Maps out data processing and contributes to DPIA documentation.

Information Security Office

- Provide technological and organizational advice.

Data Protection Officer

- Advises on DPIA necessity and measures.
- Provide feedback on DPIA reports.

Challenges and Best Practices

Challenges and Strategic Advice

Organizations often overlook DPIAs due to their complexity and the focus on more visible GDPR aspects. However, DPIAs are essential for managing privacy risks.

The challenge lies in coordinating teams, consulting authorities, and integrating DPIA outcomes into operations. Automating the DPIA process can streamline efficiency, reduce bottlenecks, and ensure timely compliance.

Strategic planning, technology integration, and cross-departmental collaboration are key solutions to overcoming DPIA challenges effectively.

Best Practices for Conducting Effective DPIAs

- Engage data subjects in the DPIA process through consultations or feedback mechanisms to understand their concerns and develop risk management strategies accordingly.
- Maintain detailed documentation of the DPIA process including scope data mapping, risk assessment, and management strategies.
- Consult data protection authorities depending on the nature of the processing activities.
- Embedded DPIA as an ongoing practice to address privacy considerations throughout data processing activities.
- Maintain transparency by providing clear information about processing activities to data subjects and stakeholders.
-

Conclusion

DPIAs are important in safeguarding personal data and ensuring global compliance with privacy regulations like GDPR.

It can be derived from this article that organizations should integrate DPIAs into their workflows by assigning responsibility, creating checklists, and including DPIAs in project planning.

The challenges explored in this article are regarding complexity and coordination which can be mitigated by adopting the best practices like engaging data subjects, consulting authorities, and maintaining detailed documentation etc.

Taking a proactive stance on DPIAs within data governance strategies is crucial. It mitigates risks, ensures legal compliance, builds trust, and improves operational efficiency.

Therefore, embracing DPIAs proactively is key to responsible and effective data management.

References

1. Data protection, Data Protection Impact Assessments (2018) Data Protection Commissionhttps://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments.
2. EDPS (2022) Data Protection Impact Assessment (DPIA) European Data Protection Supervisor https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en.
3. ICO (2022) How do we do a DPIA? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/.
4. Wolford B (2018) Data Protection Impact Assessment (DPIA) - GDPR.EU https://gdpr.eu/data-protection-impact-assessment-template/.
5. RUG (2022) Guidance document: DPIA process in research, roles and tasks (2022) https://www.rug.nl/digital-competence-centre/privacy-and-data-protection/gdpr-research/documents/guidance-dpia-process-in-research-roles-and-tasks.pdf.