DATA PROTECTION COMMISSION

www.dataprotection.org.gh

INTRO PAGE:

Welcome to the Data Protection Impact Assessment (DPIA) Unit of the Ghana Data Protection Commission (DPC). Our goal is to provide organizations with the necessary tools and guidance to adequately identify, assess, and mitigate the levels of personal data risk generated as a result of the personal data processing activities, undertaken by their various projects. These projects and their applicable documentations are reviewed by the unit and management to ensure compliance with the Data Protection Act, 2012 (Act 843) while safeguarding individuals' privacy and personal data.

Upon completion of the review of the submitted documents, organizations are given a determination from the Executive Director in order to comply with legal requirements but also foster trust and transparency within the organizations in relation to their personal data processing.

Together, we can ensure that data protection is integrated into the core of organizational practices, promoting a culture of accountability and respect for individuals' rights. For further assistance or inquiries, please do not hesitate to contact us impactassessment@dataprotection.org.gh .

DPIA FAQs

(Add the information below as a link to read more about DPIA)

What is a DPIA and Why is it Important?

A DPIA helps organizations identify and assess the potential risks to individuals' privacy and personal data protection before beginning or updating any data processing activities. It is a proactive measure to ensure compliance with legal requirements, mitigate risks, and build trust with individuals whose data is processed.

Key Benefits of Conducting DPIAs:

- **Compliance with Legal Requirements**: Ensures that organizations comply with data protection laws such as Act 843 and other laws across the world
- **Risk Management**: Proactively identifies potential privacy risks and helps mitigate or eliminate them before they materialize.
- **Protection of Individuals' Rights**: Ensures respect for individuals' privacy rights and freedoms.
- **Improved Transparency and Accountability**: Demonstrates organizational commitment to data protection and builds trust with data subjects.
- **Enhanced Data Protection Practices**: Improves organizational data protection practices by integrating privacy considerations from the outset.

Steps to Conduct a DPIA

The following steps are involved in conducting a DPIA under the **Data Protection Act, 2012 (Act 843)**:

Step 1: Identify the Need for a DPIA

Before carrying out a DPIA, assess whether the data processing activity is likely to result in high privacy risks to individuals. This could include new projects, systems, or initiatives that involve personal data, particularly if they involve sensitive or large-scale data processing. Is it a regulatory requirement? Will there be cross-border processing?

Step 2: Describe the Data Processing Activity

Provide a detailed description of the processing activities, including:

- The purpose(s) of processing personal data
- The type of personal data being processed
- The categories of data subjects involved (e.g., customers, employees)
- The intended recipients of the data
- How long the data will be retained
- The measures taken to protect the data

Step 3: Assess Privacy Risks
Identify potential risks associated with the processing, such as:

- Unauthorized access to personal data
- Data breaches or loss of data integrity
- Risk of discrimination, identity theft, or harm to data subjects
- Impact on data subject rights (e.g., right to erasure, data access)

Step 4: Evaluate Mitigating Measures
For each identified risk, assess how it can be mitigated. These measures may include:

- **Technical measures** like encryption, pseudonymization, and secure data storage.

- **Organizational measures** like staff training, access controls, and data handling protocols.
- **Policy measures** like clear data retention policies and transparency about data processing.

Step 5: Consultation with the Data Protection Commission (DPC)
If the risks to privacy are still high after implementing mitigating measures, consult with the **Data Protection Commission (DPC)** before proceeding with the processing. The DPC can provide guidance and assess whether the processing activity can proceed as planned or if further adjustments are necessary.

Step 6: Document the DPIA Process
Record the DPIA process thoroughly, including:

- The purpose of the processing
- Identified risks and mitigation actions
- Decisions made during the process
- Any consultations with the DPC
- A summary of the outcome and actions taken

Step 7: Monitor and Review
A DPIA is not a one-time exercise. Continuous monitoring and periodic reviews of the data processing activity should be carried out to ensure that it remains compliant with data protection principles and that new risks are identified and mitigated as necessary.

DATA PROTECTION COMMISSION

www.dataprotection.org.gh

When to Conduct a DPIA

A DPIA should be conducted in the following cases:

1. **Starting a new data processing activity**: If the processing could result in high risks to individuals' privacy (e.g., large-scale data collection or use of sensitive data).
2. **Introducing new technology or systems**: If new technologies, such as AI or facial recognition, could impact data security or privacy.
3. **Making significant changes to existing processing activities**: If changes may increase privacy risks (e.g., altering the scope, purpose, or context of data processing).
4. **When required by law**: For high-risk processing activities such as profiling, automated decision-making, or processing sensitive personal data.

Consider the following **Nature of Change/Project** with regards to personal data processing:

1. Procurement of New IT System: the acquisition of a completely new IT system.
2. Design and Build of New IT System: designing and developing a new IT system from scratch.

3. Change/Update to Existing IT System: Updates or modifications to an existing IT system to improve functionality or meet new needs.
4. New Business Process: Introducing a new business process that will affect how the organization operates.
5. Change to Existing Business Process: Modifications to an existing business process for efficiency, cost savings, or compliance.
6. Existing Personal Data Being Used for New Reason: Reusing personal data for a purpose other than originally intended.
7. New Personal Data Being Collected: Collecting new types of personal data from individuals.
8. New Supplier Being Appointed to Provide a New Service to Organization: Engaging a new supplier to provide services previously not available.
9. New Supplier Being Appointed to Replace an Existing Service Provided by another Supplier/In-house: Replacing an existing service provider, either an in-house service or a supplier, with a new one.
10. New Website or Website Process: The creation of a new website or implementation of new processes on an existing website.
11. Other: Specify any other nature of the change or project that does not fall under the above categories.