DATA PRIVACY IMPACT ASSESSMENT PROCEDURE

SUMMARY

This procedure addresses the data privacy impact assessment ("DPIA") process.

Each unit is responsible to:

- Ensure business managers and tech teams attend DPIA training
- Contact the PDP Team early to find out if a DPIA is needed for a new process or system
- Complete the required DPIA questionnaire
- Manage identified data privacy risks
- Update the DPIA & notify the PDP Team when the process, system, or data changes

FREQUENTLY ASKED QUESTIONS

1. What is a DPIA?

A Data Privacy Impact Assessment starts with a questionnaire that is used to evaluate risks associated with collecting, using, and sharing personal data. It is designed to ensure data privacy risks to individuals are timely identified and mitigated.

2. What criteria trigger the need for a DPIA?

Personal data access, collection, use, storage, retention, or transfer involving:

- Sensitive Personal Data (e.g., biometrics, health, religion)
- Combining multiple datasets
- New or emerging technology
- Vulnerable groups (e.g., children)
- Monitoring, surveillance, or tracking
- Automated decision-making without human review
- Likely significant harm to an individual's privacy

3. At what stage should the DPIA process begin?

Before any processing begins—or as early as possible in procurement, contracting, or system design—to avoid delays and unnecessary risks.

4. What are the steps to complete a DPIA?

1. Contact the PDP Team to determine if a DPIA is required.
2. Complete the questionnaire or template provided.
3. Meet with PDP Team to review responses and to consult InfoSec on safeguards.
4. PDP Team issues a report identifying risks and recommendations.
5. Manage identified risks
6. Update the DPIA if the process, data, or system changes.