Data Protection Impact Assessment Process (June 2023)

1. **Data protection impact assessments (DPIA)**
   Also known as privacy impact assessments (PIAs), DPIAs are performed to identify, analyze, and minimize the data protection risks of a project or plan involving personally identifiable information (PII) or other protected data identified in the organization data classification policy.

   Risks to personal information, etc., can include anything from unauthorized access by internal or external entities to not overseeing personal data according to the data subject's rights. A DPIA should result in a list of measures the organization will take to address the identified risks.

   Incorporate DPIAs in new projects involving personal data and use them throughout planning and development.

2. **DPIA Guidelines**
   a. *Evaluation Or Scoring:* The organization must conduct DPIAs when evaluating people, especially their work performance, economic situation, health, personal preferences or interests, behavior, location, or movement. Privacy Regulations also require DPIAs for credit score determinations, genetic testing to assess health risks, and behavioral-based marketing profiling.

   b. *Automated Decision-Making:* DPIAs are necessary when enacting processes that automate legal decision-making. The organization must ensure that such processing does not exclude or discriminate against individuals.

   c. *Systematic Monitoring:* The organization must conduct DPIAs when observing, monitoring, or controlling data subjects, including when they are in public areas.

   d. *Sensitive data handling*: DPIAs are needed whenever the organization deals with highly personal data, such as a patient's health data.

   e. *Large-Scale Data Processing:* DPIAs are required when organizations implement large-scale data processing. Criteria for determining whether data processing occurs on a large scale include the number of data subjects and the duration and geographical extent of the activity.

   f. *Matching Or Combining Datasets:* The organization must conduct a DPIA when merging or comparing two or more sets of data collected for different purposes.

   g. *Vulnerable Data Subjects*: DPIAs are required when there is a power imbalance between data subjects and the data controller since that could harm the data subject. They are also necessary for data subjects who cannot oppose the processing of their data, such as children, employees, and people with mental illnesses or cognitive issues.

   h. *Innovative Use*: DPIAS are required for newer technologies, such as IoT devices, fingerprint scanners, and facial recognition systems.

   i. *Transfer of Data Outside the EU or UK:* When transferring data outside the EU or UK, the organization must perform DPIAs to ensure appropriate safeguards are in place.

   j. *Handling Applicant Data:* When an organization conducts processes that prevent data

subjects from exercising a right or using services or contracts, it must perform a DPIA.

3. DPIA Assessment Requirements

The following requirements direct processors on their exact conduct once the DPIA begins, which supports the ability to comply with Privacy Regulations requirements and includes:

- *Risk identification:* Define how to consult with processors to understand risks before processing commences. Ensure that the extent of processing matches the overall purpose. Once risks are assessed, include written measures on how to measure and mitigate them.
- *Stakeholder list:* Identify all key stakeholders and plan to communicate and update them at various stages.
- *Decision-making records:* Include detailed documentation on who is consulted before and during processing and who has access to the data. Additionally, document all processing methods, any technology used, and any changes in methodology.
- *Review processes:* As the DPIA is conducted, create a schedule to review the project status and alterations constantly. Remember, any changes in the assessment nature, context, scope, or design may require restarting the process from the beginning.

4. DPIA Functional Steps

a. Identify the need for a DPIA. Be sure to document the following aspects of the processing:
   - Nature — What do you plan to do with the data?
   - Scope — What data will be processed?
   - Context — Internal and external factors that could affect expectations or impact.
   - Purpose — Why your organization wants to process the data.

b. Describe processing operations and their purpose. Document how data will be processed throughout the project and the scope of the data with the following questions:
   - How is data being collected and used?
   - Where and how is data being stored?
   - Where is data being collected from?
   - Is the data stored with any third or other downstream parties?
   - Are there any high-risk data categories involved?
   - How much data is being collected, and how many data subjects are impacted?
   - Where are data processing activities taking place?
   - What are the data retention requirements?

c. Assess necessity and proportionality. Justify the data processing activities that occur by explaining what is required for the objectives and outcomes of the project. Start by answering these questions:
   - Is there a legal basis for collecting this data?

- Are appropriate consent measures in place?
- Are vulnerable data subjects involved?
- Have previous projects of a similar nature performed similar processing? Were security flaws identified and remediated?
- Is data processing necessary to achieve the objectives of the project?
- How are consumer rights being upheld?
- Are there ways to minimize the use of consumer data?

d. Consult interested parties. Consult several key parties throughout the course of the DPIA. These include:

- *The Data Protection Officer (DPO) or similar role*: The organization's DPO is responsible for monitoring compliance with the Privacy Regulations and other data protection laws, training staff in data processing, and acting as a contact point for the data subjects. Consulting a DPO can help you demonstrate compliance, increase accountability, and obtain feedback on project risks.
- *Project Stakeholders:* Involving all stakeholders will help you fully understand the extent and necessity of data processing activities and devise appropriate strategies to address risks.
- *Data Subjects and Their Representatives* — Data subjects and their representatives can give you feedback on how their data is processed and ensure the legality of your processing activities.
- Outside Experts: For data privacy expertise, consider engaging outside experts such as information security professionals, lawyers, technologists, and security analysts.

e. Identify and Evaluate Risks to Personal Data et al. Create a prioritized list of assets and identify potential vulnerabilities. In your risk analysis, consider:

- Data whose loss or exposure would impact operations.
- Key business processes that use those data assets
- Whether data is being anonymized
- Whether data retention policies are applicable
- Whether data is being stored in unsafe locations or could be moved to such locations
- Whether the scope of data processing will change throughout the course of the project
- Whether appropriate access controls are being applied
- Threats that could impair the organization's ability to operate and the severity and likelihood of each threat.

f. Identify Measures to Address Risks. Once you have a good idea of the potential risks involved in the project, strategically formulate and implement appropriate risk mitigation measures. Data security solutions can help you ensure that:

- The necessary security measures are in place to prevent unauthorized access to personal data by internal or external actors.

- Data retention policies are in place to remove data that no longer requires them.
- Discovery and monitoring technologies provide visibility into where personal data exists, who is accessing it, how it is being used, and how it moves throughout the organization.
- Remediation actions (such as deleting unnecessary data and cleaning up access) can be automated and performed at scale.
- It is imperative to document which information protection risks a specific mitigation measure will help address and how.

g. Get sign-off. Once all risks are identified and an appropriate security strategy is devised, obtain sign-off for implementation from relevant parties. The list will depend on the organization and specific project but often includes the Data Protection Officer and management team members.

h. Implement measures to address risks. Deploy the solutions and other measures identified to reduce risks.

i. Produce a final DPIA report. It must include the following information:
   - A detailed description of the project and its purpose
   - An assessment of data processing needs and scope.
   - An evaluation of data protection and consumer privacy risks
   - An explanation of how the organization will mitigate risks and comply with Privacy Regulation requirements.

Publish DPIAs to appropriate stakeholders in and outside the organization.