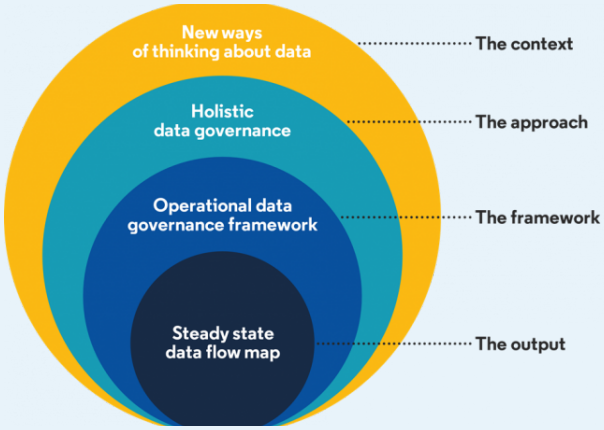
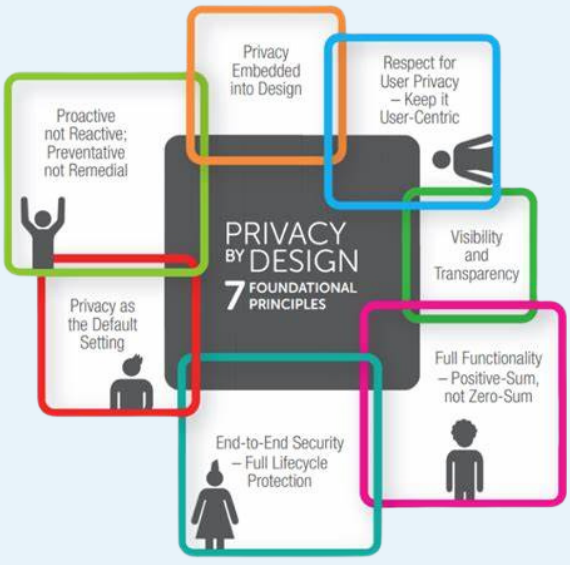
PRIVACY BEST PRACTICES

HOLISTIC DATA GOVERNANCE

A holistic approach to data governance aligns the top-down focus, common to traditional governance models, with an operational and bottom-up view. The result is a holistic view of data governance that extends across the entity to bring value to each perspective independently, while complementing and enhancing the others. Steady state data flow mapping can support holistic governance.



Tip: Consider a Steady State data flow mapping strategy that helps to make data governance relevant to the operational staff at your entity. Contact PrivCom to learn more about the 4-step Steady state data flow mapping process.



PRIVACY BY DESIGN & DEFAULT

Privacy by Design means privacy is integrated into products, services, and system designs by default. Privacy by Design is a holistic approach to privacy based on seven foundational principles, including the need to act proactively and preventatively rather than reactional and remedially. More individuals understand the value of their data which means that entities will need to provide additional assurance by making Privacy by Design so by default, their operation conditions will ensure privacy and give users more control over their data.

MINIMISATION

The principle of data minimisation involves limiting data collection to only what is required to fulfill a specific purpose.

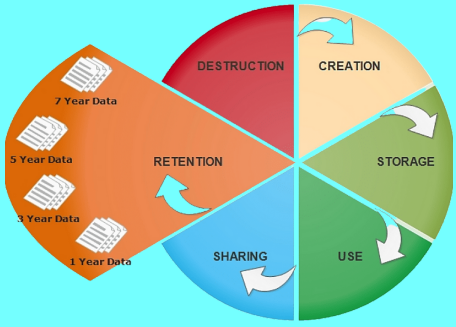
DESTRUCTION/DISPOSAL

When an organisation no longer has a Condition under PIPA for using information, the information must be securely destroyed and disposed of.

RETENTION

Data retention is the practice of preserving data for a specific period of time to meet technical, business, or regulatory requirements.

The simplest and best data retention strategy is to avoid storing any information that you don't need. If information doesn't exist, it doesn't require a flow diagram, isn't subject to regulation, and never will have to be deleted.

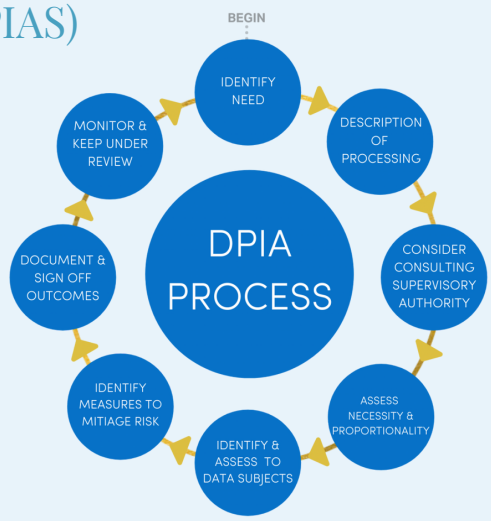


PRIVACY COMPLIANCE TOOLS

DATA PRIVACY IMPACT ASSESSMENTS (DPIAS)

Data Privacy Impact Assessments (DPIAs) go beyond assessing compliance with technical requirements by evaluating the inherent privacy risks to individuals and determining the sufficiency of the control for mitigating those risks.

DPIAs empower entities to examine whether the processing of information will create value for society and individuals.



TRANSFER IMPACT ASSESSMENTS (TIAS)

With developments in global communication and business processes continuing to evolve at a rapid speed, global data privacy & protection regulatory changes can seriously affect entities of all sizes locally and anywhere in the world. Transfer Impact Assessments (TIAs) have become a recommended best practice. Contact PrivCom for support with TIAs.

RECORDS OF PROCESSING ACTIVITIES (ROPAS)

Every entity should have, for its own purposes, an accurate picture of all the information it controls and/or uses, through regular data mapping exercises.

Keeping a RoPA up to date can assist with meeting privacy compliance standards across the board.

The Conditions under Bermuda's PIPA (Article 6) for all information uses should be accounted for in detail on a RoPA, as well as all information relating to special category or criminal defense data.

A RoPA should provide access to additional details wherever possible, such as records of consent, descriptions and copies of relevant contracts or agreements, privacy notices, histories of data breaches, and any other information relating to personal information that might provide an additional measure of depth and transparency to the RoPA.

Example of key elements in a RoPA

Function	Purpose of Processing	Joint Controller (if applicable)	Categories of Individuals	Categories of Personal Data	Category of recipients (if applicable)	Retention schedule
Contact	School use		Current Pupils	Contact details	Destination school	Duration of attendance at school
Care	Care		Current Pupils	Medical needs/history	Destination school	Duration of attendance at school
Learning	Learning		Current Pupils	Performance outcome	Destination school	Duration of attendance

Best practice tip:
A RoPA should contain the name and contact of the entity, as well as all parties involved in the handling of information, and their corresponding relationships. It should also provide reasons and methods for using all personal information, as well as any transactional history.

ENGAGE WITH US!