Annex G- Vendor Privacy Considerations

(Land Title and Registration Department's Proponent Privacy Assessment)

On the 1 January 2025, the Personal Information Protection Act, 2016 ("PIPA"), came into full force and effect in Bermuda. This Act binds all government departments including the LTRO, therefore all proponents must be knowledgeable of the obligations that PIPA places on the LTRO and factor them into the solution proposed.

Shortlisted proponents must be prepared to demonstrate the integration of the privacy considerations outlined below in the proposed solution during the demonstration and oral presentation.

Establishing the Key Facts
The key applicable terms under PIPA are stated below. :

- **What is personal information?** Under PIPA, personal information is any information about an identified or identifiable individual. For example: name, ID number, location, IP address; biometric data, CCTV image etc.

- **What are the categories of personal information?** There are two main categories under PIPA. The first is 'personal information', which is generalised term for any information relating to an identified or identifiable individual. The second is 'sensitive personal information' which is a subset of personal information and includes an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information. All the rules that apply to personal information also apply to sensitive personal information.

- Additional rules apply only to sensitive personal information. Please also note that a third category also exists that may be defined as non-statutory sensitive personal information. This is personal information that is sensitive due to its context i.e. the name and address of an abused wife who is hiding from her abusive husband.

- **What are the conditions for using personal information?** There are several direct conditions in s6(1) PIPA which provide a lawful basis for using personal information. They are:

a) Consent.
b) A reasonable person would not object and the use does not prejudice the individual's rights (this basis is not available for sensitive personal information).
c) Contractual obligation.
d) Legal obligation.
e) Publicly available personal information and its use is consistent with its availability.
f) Emergency threatening life health or security.
g) Public interest.
h) Necessary for employment.

The Land Title and Registration Act 2011 provides the legal bases for the use and collection of personal information by the LTRO. The LTRS will collect personal and sensitive personal information for the purposes of land title registration services, deeds registry recording, facilitating payment of registration fees, the creating of user profiles, identity verification, contact information for the service of notices and general communication with the LTRO. The operations to be performed on the personal information by the LTRS includes collecting, organizing, storing, using. The LTRO is allowed to collect the personal and sensitive information in the public interest and the records of the LTRO are considered to be public records. The LTRO will from time to time need to verify the identity of an individual however and the identification information issued to the LTRO does not form a part of the public records. It is imperative that the LTRO accounts for its use, storage and handling of personal and sensitive personal information.

The LTRS will interact with the following personal information

1. Property owner names and addresses
2. Transaction details including purchase prices,
3. Mortgage information such as Mortgage rates
4. Legal documentation
5. Historical deed information
6. Contact details of property owners and legal representatives
7. Contact information, Home Address and Personal email, Phone numbers
8. Commercial information
9. Records of personal properties
10. Signatures

The LTRS will interact with the following sensitive personal information:

1. Nationality/ immigration status

2. Marital status and family relations

The proponent must be prepared to explain the security measures which ensure that personal and sensitive data is not shared or processed in a way that is incompatible with the reason for which it was given to the LTRO. In response to this section the proponent should demonstrate that the utilization and transfer rights will be restricted, quality assurance revisions will be in place for compliance in software development. Regulated procedures must be in place for purpose amendments. The LTRS must have differentiated access rights based on internal roles and differentiated access rights based on external user profiles. Access rights are to be differentiated on the basis of identity, management role and purpose. The LTRS must have secure authentication methods in place. For example statistical metrics of current mortgages should be available to the class of Bank users but not users who are members of the general public. The LTRS should feature pop up consent/acknowledgment selections to privacy terms and conditions.

The LTRS must contain privacy tools and settings namely the ability to request for portions of documents to be redacted. The interface must be clear, conspicuous and user-friendly. Hyperlinks to the processing procedure and comprehensive privacy notice must be conspicuous on all external user profiles. The processing procedure outlining the purpose specification for information collection as well as the comprehensive privacy notice will be provided by the LTRO.

The LTRS must have a user-friendly mechanism to update simple personal information such as a change of address. The workflow, application type and details to facilitate the updating of simple personal information will be provided by the LTRO.

It is anticipated that this project, and service will involve the transfer of information to external third parties. Namely the proponent, suppliers, processors, contractors. The proponent will be required to give a listing of personnel by role who will manipulate and interact with any personal and sensitive data collected by the LTRS or forwarded to the proponent to facilitate the construction of the solution.

There is no retention period for personal and sensitive personal information collected by the LTRO as records are required to be held indefinitely. The security and hosting components of the system must address the privacy considerations outlined above.

Proponents should address the questions below in their submission.

For the purposes of this document, we will use the following terms:

Controller – the organization that dictates the use of the personal information.

Processor – the organization that uses the personal information to the order of a controller.

General Questions:

- Is the proponent a controller or processor for the services being provided?
- Does the proponent have a privacy documentation you can review?
- Does the vendor have verifiable privacy certifications or trust marks? Examples of appropriate certification include:
    - ISO 27001 Certification
    - ISO 27002 Certification
    - BS 10012 Certification
    - SOC 2 Type I Report
    - SOC 2 Type II Report
    - SIG Questionnaire
    - CSA CAIQ
    - CSA STAR
    - Approved Code of Conduct
    - Approved Certification Mechanism
    - Security Whitepaper
    - Not applicable
    - Other
- Is anything about the proponent's platform or service overly intrusive or prone to mission creep?
- Does the proponent have privacy professionals on staff? Are they qualified? What experience do they have?
- Who will have access to personal information? (i.e. service individuals only?)
- Does the proponent have security to prevent access by non-service individuals?
- What security controls does the proponent have in place?
- Does the proponent have good privacy-by-design so that default settings favor privacy?
- Does the proponent have an incident response and recovery plan?
- What privacy audit requirements does the proponent have?

- What is the reporting line for privacy matters within the proponent? (i.e. if a company is a Board member responsible for privacy matters).
- What privacy training does the proponent give its staff?
- Does the proponent have a security breach register, and can you view this?
- Does the proponent employ the use of subcontractors are used or not and for what purpose?
- Does the proponent meet a recognized security standard?
- Does the proponent have a security policy?
- What checks/vetting does the proponent have on staff members?
- What access will be provided for us to audit their privacy compliance regime?
- Does the proponent have penetration test reports?
- Has the proponent been involved in past litigation and settlements re service offering?
- What is the proponent workplace culture like? Unfair working practices / bias / discrimination / employee retention rate? (goes to potential breaches triggered by aggrieved staff members).
- What is the proponent disaster preparedness plan?
- What is the proponent Business continuity plans/recovery plan?
- Has the proponent provided a solution in a jurisdiction with comparable privacy legislation? (Please see the list of comparable Jurisdictions below.)

Comparable Jurisdictions:

Member States of the EU:	**States of the European Free Trade Association:**
Austria	Iceland
Belgium	Norway
Bulgaria	Liechtenstein
Croatia	
Cyprus	**United Kingdom of Great Britain and Northern Ireland**
Czechia	
Denmark	**Jurisdictions with 'adequate' laws**
Estonia	Andorra
Finland	Argentina
France	Faroe Islands
Germany	Gibraltar
Greece	Guernsey
Hungary	Isle of Man
Ireland	Israel
Italy	Jersey
Latvia	New Zealand
Lithuania	Republic of Korea
Luxembourg	Switzerland
Malta	Uruguay
The Netherlands	
Poland	**'Adequate' laws, subject to limitations**
Portugal	Canada
Romania	Japan
Slovakia	
Slovenia	
Spain	
Sweden	

Questions specific to Cloud Services

- What is the Cloud Service name?
- Cloud Service Provider (legal entity under the contract)
- What type of cloud service is involved and under which delivery model will the service be delivered?
- Which system (s) will the cloud service in question support?
- What processing activity(s) will be performed using the cloud service?
- Are there suitable policies and procedures in place to ensure privacy compliance with PIPA and the privacy/data protection requirements of the cloud location?
- Please include a mapping of all third-party/sub-processors and provide documentation of assessments to indicate that PIPA and other requirements (security, back-ups, replication, destruction, agreements, etc.) are met.
- Are there established procedures etc. for (possible) notifying the Government of Bermuda of possible security breaches as well as assistance in notifying the Government of Bermuda of breaches of personal information?
- Can they delete or return personal information and/or other data at the end of the agreement?
- Are there any threats to confidentiality in that the cloud supplier may have to transfer personal information to third countries on the basis of a court order or request against their parent company?
- If personal information is processed in or from third countries, are we able to instruct the cloud provider which countries are permitted and which they should not go to?
- Are there conditions in the countries where they provide their cloud(s) that affect the effectiveness of our transfer basis, and can they be brought up to PIPA requirements?
- Any contractual agreement with the Government of Bermuda will include the legal requirements, contractual clauses or otherwise, to ensure that the transfers from Bermuda to the third country meet PIPA requirements.