Cayman Islands Government

Department of Planning and Associated Statutory Bodies

(CPA, DCB, BB, EBE)

Data Protection Policy

Version: 1.0

Initial release date: 01 June 2024

Date of current version: 01 June 2024

Document Administration

Document location:	DoP website (https://www.planning.ky/data-protection-policy)
Document name:	Department of Planning Data Protection Policy

Revision Record

Version	Date	Revision Description	Author
1.0	01 June 2024	Initial approved document issued	Data Protection Leader - KT

Version Control Notice:

This document is a controlled document that supersedes all previous versions. Please discard any previous copies of this document dated prior to the version and publication date noted above this page.

Anyone who obtains an electronic or printed version of this document is responsible for ensuring that they have the latest version. The latest version of this document is available on the Planning website (https://www.planning.ky/) and can also be obtained by email on request to info@planning.gov.ky.

Table of Contents

1. EXECUTIVE SUMMARY

This Data Protection Policy ("this Policy") establishes how the Department of Planning and associated statutory bodies protects Personal Data based on the Cayman Islands Data Protection Act (2021 Revision) ("DPA") and Data Protection Regulations, 2018 ("Regulations") and in line with the **Cayman Islands Government ("CIG") Privacy Policy**.

This Policy ensures the Department of Planning's employees and other Public Officials and Suppliers who have access to Personal Data processed by the Department of Planning and associated statutory bodies understand the rules governing the use of Personal Data.

2. INTRODUCTION

2.1 Background

When delivering public policies, programmes and services, the Department of Planning and associated statutory bodies may collect, store and use Personal Data, including but not limited to Personal Data relating to individuals residing in the Cayman Islands, visitors to the Cayman Islands, Civil Servants, other Public Officials, affiliates, and Suppliers and service providers. In most cases, the Personal Data Processed by the Department of Planning and associated statutory bodies will be provided directly by the individual (i.e. the Data Subject). However, the Department of Planning and associated statutory bodies may also receive Personal Data indirectly (e.g. when conducting a background check or from another Public Authority in the course of their duties).

The Department of Planning and associated statutory bodies must only use Personal Data to deliver public policies, programmes and services, including under enabling legislation, and for other legitimate purposes. The Department of Planning and associated statutory bodies are responsible for the protection of Personal Data under its control and compliance with applicable privacy laws, including the DPA and Regulations, and the CIG Privacy Framework

2.2 Purpose and Objectives

Implementing and complying with this Policy will enable our success by maintaining the public's trust in the handling of Personal Data to make the lives of those we serve better. It aims to minimise risk of breach of privacy laws and any resulting complaints and/or enforcement action, including monetary penalties.

The objectives of this Policy are to:

a. facilitate statutory and regulatory compliance by the Department of Planning and associated statutory bodies in accordance with applicable legislation;
b. promote consistency in practices and procedures in administering the **CIG Privacy Policy**; and
c. ensure effective protection and management of Personal Data throughout its collection, use, disclosure, retention and disposal.

2.3 Scope

This Policy applies to the Department of Planning, all Data Processors engaged by the Department of Planning, the Central Planning Authority, the Development Control Board, the Builders Board, and the Electrical Board of Examiners. This Policy applies to all employees of the Department of Planning, all members appointed to theses associated statutory bodies, all other Public Officials, Suppliers and service providers that Process Personal Data on behalf of or that have access to Personal Data where the Department of Planning, or one of its associated statutory bodies is the Data Controller, a Joint Data Controller, or a Data Processor. This Policy must be read in combination with all legislation relevant to the Department of Planning and associated statutory bodies; all relevant CIG policies and procedures; and all policies, procedures and other documentation specifically relevant to data protection in

the Department of Planning and associated statutory bodies, including Privacy Notices, MOUs, Data Processing Agreements and Terms of Service.

This Policy covers the operations of the Department of Planning, Central Planning Authority, Development Control Board, Electrical Board of Examiners, Builders Board but does not cover the operations of the National Conservation Council and the Health Practice Commission. Therefore, in **Section 6 Policy Requirements**, "Department of Planning" must be read to include each of these associated statutory bodies that is within the scope of this Policy.

Please see the following additional Data Protection documents as required:

1. The Department of Planning External Privacy Notice
2. The Department of Planning Cookie Notice

3. ENABLING LEGISLATION AND KEY POLICIES

The DPA along with the Regulations serve as the key enabling legislation for this Policy. As a Public Authority, the Department of Planning is also subject to the National Archive and Public Records Act (2015 Revision) read with the National Archive and Public Records Regulations, 2007; the Public Service Management Act (2018 Revision) read with the Personnel Regulations (2022 Revision); and other legislation.

In addition to CIG policies that together form the CIG Privacy Framework, this Policy must be read along with the following enactments and Department of Planning policies:

1. Development and Planning Act (2021 Revision)
2. Development and Planning Regulations (2022 Revision)
3. Building Code Regulations (2021 Revision)
4. Development Plan Planning Statement, 1997
5. The Builders Act, (2007 Revision)
6. The Builders Regulations, (2008 Revision)
7. Electricity Act (2008 Revision)
8. Electricity Regulations (2011 Revision)
9. Water Authority Act (2022 Revision)
10. Water Authority Regulations (2022 Rev.)

See also **CIG Privacy Policy Appendix B: Key Legislation, Policies and Resources**.

4. DEFINITIONS AND ABBREVIATIONS

The ***Department of Planning*** (DoP): The Department of Government which is established in accordance with section 3A of the Development and Planning Act (2021 Revision) and is a Data Controller in relation to the Processing of Personal Data as noted in section 2.3 of this Policy.

The ***Central Planning Authority*** (CPA): The Public Authority which is established in accordance with section 3 of the Development and Planning Act (2021 Revision) and is a Data Controller in relation to the Processing of Personal Data as noted in section 2.3 of this Policy.

The ***Development Control Board*** (DCB): The Public Board which is established in accordance with section 3 of the Development and Planning Act (2021 Revision) and is a Data Controller in relation to the Processing of Personal Data as noted in section 2.3 of this Policy.

The ***Builders Board*** (BB): The Public Board which is established in accordance with section 4 of the Builders Act (2007 Revision) and is a Data Controller in relation to the Processing of Personal Data as noted in section 2.3 of this Policy.

The ***Electrical Trade Licensing Board of Examiners*** (EBE): The Public Board which is established in accordance with section 6 of the Electricity Act (2008 Revision) and is a Data Controller in relation to the Processing of Personal Data as noted in section 2.3 of this Policy.

This Policy must be read with the **CIG Privacy Policy**. Key data protection terms and abbreviations, including those which are capitalised throughout this Policy, are defined in the DPA and/or in section 4 of the **CIG Privacy Policy**.

5. ROLES AND RESPONSIBILITIES

Data protection roles and responsibilities across the CIG are outlined in section 6 of the **CIG Privacy Policy**. See also **CIG Privacy Policy Appendix C: RASCI Matrix** for a complete table that defines the persons who are Responsible, Accountable, Supporting, Consulted and Informed ("RASCI") in relation to specific data protection activities.

6. POLICY REQUIREMENTS

6.1 Data Protection Principles

6.1.1 The Department of Planning and associated statutory bodies are each Data Controllers, having determined the purposes, conditions and manner in which Personal Data are Processed. Data Controllers are responsible for complying with the DPA, including the Data Protection Principles, in relation to these Processing activities. **Section 2.3 Scope** sets out the scope of this Policy and provides that "Department of Planning" should be read in this **Section 6 Policy Requirements** to also include the associated statutory bodies listed there.

6.1.2 The Data Protection Principles define the Department of Planning's responsibilities in protecting Personal Data. All Department of Planning employees and all other Public Officials (including members of boards and committees) and Suppliers that have access to or Process Personal Data on behalf of the Department of Planning must handle Personal Data in alignment with these principles.

6.1.3 To ensure the obligations under the DPA are met, the Processing of Personal Data must comply with the principles of the DPA, unless limited exceptions and exemptions apply. Accordingly, Personal Data will be:

a. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;
b. Collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected or further Processed;
d. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that Inaccurate Personal Data, having regard to the purpose for which they are Processed, are rectified, blocked, erased or destroyed without delay;
e. Kept for only as long as it is needed and subsequently destroyed; The Department of Planning will ensure the purposes of Processing clearly include the legal obligation the Department of Planning has as a public agency to maintain public records in accordance with the National Archive and Public Records Act (2015 Revision) and to only destroy public records in accordance with an approved disposal schedule;
f. Processed in accordance with the rights of Data Subjects, including under the DPA;
g. Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and
h. Transferred only to countries or territories which ensure there is an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

6.2 Legal Bases / Conditions of Processing

6.2.1 It is the Department of Planning's responsibility to understand the different legal bases for Processing Personal Data and ensure the Department of Planning has a legal basis for Processing Personal Data and an additional legal basis for Processing Sensitive Personal Data. Some legal bases have different

requirements depending on the purpose of collection. The requirement to have a legal basis or legal bases for Processing applies to the disclosure of Personal Data as well as to providing access to Personal Data between the Department of Planning and other Data Controllers, including other Public Authorities.

6.2.2 The Department of Planning shall ensure that one or more legal bases will be satisfied whenever Personal Data are Processed. The Department of Planning shall identify and document the legal basis or legal bases relied upon in relation to the Processing of Personal Data and Sensitive Personal Data for each specific purpose or group of related purposes. This will be documented in the Department of Planning External Privacy Notice located on the planning website (https://www.planning.ky/).

6.2.3 The Department of Planning shall ensure that the legal basis or legal bases for Processing of Personal Data and Sensitive Personal Data are identified in advance and that all Processing of Personal Data and Sensitive Personal Data complies with the DPA.

6.2.4 The Department of Planning shall document and review the legal bases of its Personal Data and Sensitive Personal Data Processing activities, including any information that may be recorded in RoPAs, this Policy, Privacy Notices, MOUs and other documentation (if applicable), at appropriate intervals to ensure compliance with the DPA and promote accountability.

6.3 Purpose Limitation and Data Minimisation

6.3.1 The Department of Planning shall clearly identify and document the purposes for Processing Personal Data.

6.3.2 The Department of Planning shall ensure that the purposes for Processing Personal Data are included in the Department of Planning's Privacy Notices. See **Privacy Notices** (section 6.6) for more details.

6.3.3 The Department of Planning shall ensure that when new purposes for Processing Personal Data are identified, the Department of Planning is satisfied that one of the following applies:

a. The new purpose is not incompatible with the original purpose; or
b. The Processing is exempt from the second Data Protection Principle (purpose limitation) pursuant to a specific provision in Part 4 of the DPA; or
c. The Department of Planning has identified the legal basis or legal bases requiring or allowing the new Processing – for example, a new legal obligation or function – and is able to ensure the Processing will be fair and in compliance with the DPA, including the Data Protection Principles.

6.3.4 The Department of Planning shall ensure the Personal Data collected or further Processed is adequate, relevant and limited to what is necessary in relation to the purposes for which the Personal Data are being Processed or will be Processed.

6.3.5 The Department of Planning shall ensure that when Personal Data are no longer needed for specified purposes, they are destroyed, secured, archived or anonymised in accordance with the **National Archive and Public Records Act (2015 Revision)** and **CIG Privacy Policy**. See **Data Retention and Disposal** (section 6.9) for more details.

6.3.6 The Department of Planning shall ensure that only the minimum amount of Personal Data needed to fulfil the purpose or purposes are requested, collected, accessed, shared, disclosed or otherwise Processed.

6.3.7 The Department of Planning shall review its data Processing periodically to check that the Personal Data the Department of Planning holds are still relevant and adequate for the purposes of Processing.

6.4 Consent

There is no hierarchy between the legal bases for Processing of Personal Data, of which a Data Subject's Consent is one option. Where there is a significant imbalance between the position of the Data Subject and The Department of Planning, Consent shall not provide a legal basis for the Processing. Where Consent is relied upon as a legal basis for Processing, it must be valid and Schedule 5 of the DPA applies. Therefore, the following must be adhered to:

6.4.1 To ensure any Consent that may be collected is valid:

a. The Data Subject must give Consent prior to the Processing;
b. The request for Consent must be in an intelligible and easily accessible form, using plain and clear language, and require the Data Subject to make a statement or to take a clear affirmative action that is separate from any declaration that may be made at the same time concerning another matter;
c. The Consent must be freely given, specific, informed and unambiguous;
d. What the Data Subject has given Consent to (i.e. the purpose(s)) must be clearly documented;
e. When and how the Data Subject has given Consent must be able to be proven;
f. The Data Subject must be able to withdraw the Consent at any time; and
g. The Processing of Personal Data on the basis of Consent must be stopped if Consent is withdrawn.

6.4.2 The declaration of Consent should be obtained in writing or electronically for the purposes of documentation. In some circumstances, and provided no other law requires written Consent for the Processing, Consent may be given verbally. The granting of Consent should always be documented in a way that will allow the Department of Planning to prove the Consent was given.

6.4.3 The Department of Planning shall implement appropriate measures where Consent from Children or other vulnerable Data Subjects is required, including verifiable Consent of the Data Subject's parent(s)/guardian(s) or age-verification and/or competence-verification measures.

6.4.4 The Department of Planning shall implement processes to review and refresh Consent at appropriate intervals, at least annually.

6.5 Privacy Notices

Under the DPA, The Department of Planning is required to provide information to Data Subjects on the purposes for which The Department of Planning Processes their Personal Data. The Department of Planning may also be required to provide additional detailed, specific information about the Department of Planning's Processing activities, including in response to a Data Subject Access Request (DSAR). The Department of Planning shall ensure that appropriate Privacy Notices are in place advising Data Subjects how and why their Personal Data are being Processed and advising them of their rights.

6.5.1 Information about Personal Data Processing must be provided through appropriate Privacy Notices, which must be concise, transparent, intelligible, easily accessible and communicated in clear and plain language.

6.5.2 Privacy Notices must contain, at minimum, the identity of The Department of Planning or relevant associated statutory body as a Data Controller and the purpose(s) for Processing the Personal Data. The purpose(s) must be described in sufficient detail as to be meaningful and understandable to the Data Subject and not overly general in nature.

6.5.3 Privacy Notices (e.g. a Cookie Notice & External Privacy Notice) for The Department of Planning shall be developed, implemented and reviewed on an annual basis or upon changes to the purposes, legislative framework (legal and regulatory), processes, procedures and/or technologies.

6.5.4 The Department of Planning shall update its Privacy Notices and communicate the changes to Data Subjects before starting any new Processing if The Department of Planning plans to use Personal Data for a new purpose that is incompatible with the original purpose.

6.5.5 Privacy Notices may also explain, among other items, the legal basis/bases for Processing the Personal Data, categories of Personal Data collected, how the Personal Data will be used, Data Subject Rights, potential Recipients of the Personal Data, applicable retention periods, security measures, etc.

6.5.6 Privacy Notices should be adapted for either written or verbal communication of key information and generally provided directly to the Data Subject at the time the Personal Data are collected, e.g. as part of an application form, an intake interview, or any other similar process.

6.5.7 Privacy Notices for Data Subjects that are not employees of the Department of Planning, including Cookie Notices, shall be published on the Department of Planning's website and shall be publicly accessible and easily identified by Data Subjects.

6.5.8 The Employee Privacy Notice shall be published or otherwise made readily available internally and shall be easily identified and accessible by all employees of the Department of Planning.

6.6 Individual Rights

The Department of Planning shall Process Personal Data in accordance with Data Subjects' rights. This means that the Department of Planning shall ensure there are measures implemented that allow individuals to exercise their rights under relevant legislation, including the DPA. Furthermore, the Department of Planning shall respect and honour these rights in compliance with applicable legislation.

In accordance with the DPA, Data Subjects have rights in relation to their own Personal Data, which include:

6.6.1 **The right to be informed**: The right of Data Subjects to obtain information regarding why and how their Personal Data are Processed by the Department of Planning, with limited exemptions.

a. The Data Subject shall receive information directly or be referred to the Privacy Notice published by the Department of Planning if the Privacy Notice provides all of the required information.

6.6.2 **The right of access**: The right to request access to the Personal Data the Department of Planning maintains on the Data Subject and to supplementary information about the Processing, with limited exemptions.

a. All the Department of Planning employees are required to be trained on how to recognise a Data Subject Access Request (DSAR) and understand when a DSAR applies.
b. All the Department of Planning employees are required to immediately report a DSAR to the Information Manager. See **Data Subject Access Requests (DSARs)** (section 6.8) for more details.

6.6.3 **Rights in relation to inaccurate data**: The right for Inaccurate Personal Data Processed by the Department of Planning to be rectified, blocked, erased or destroyed. The Data Protection Principles require Personal Data to be accurate and, where necessary, kept up to date. An order from the Ombudsman following a complaint may also require a Public Authority to rectify, block, erase or destroy Inaccurate Personal Data.

a. All the Department of Planning employees are required to be trained on how to recognise a complaint in relation to Inaccurate Personal Data and the policies and procedures the Department of Planning has in place to address Inaccurate Personal Data in the absence of an order from the Ombudsman.
b. All the Department of Planning employees are required to immediately report complaints regarding Inaccurate Personal Data to the Data Protection Leader.
c. The Department of Planning shall ensure there are processes in place to respond without undue delay to a complaint or request from a Data Subject in relation to Inaccurate Personal Data.
d. The Department of Planning shall ensure there are procedures in place to inform Data Subjects if and when the Department of Planning rectifies, blocks, erases or destroys any Inaccurate Personal Data following a complaint or request from the Data Subject or an order from the Ombudsman.
e. The Department of Planning shall ensure that when a complaint in relation to Inaccurate Personal Data will not lead to further action or a request from the Data Subject to rectify, block, erase or destroy Personal Data is lawfully denied, the Department of Planning responds to the Data Subject in a timely manner and explains the reasons for closing the complaint or denying the request.

f. The Department of Planning shall ensure Process Owners maintain an up-to-date log of complaints in relation to Inaccurate Personal Data and requests to rectify, block, erase or destroy Personal Data, where those complaints and requests relate to processes within their control.
g. The Department of Planning shall ensure the Data Protection Leader maintains an up-to-date log of orders from the Ombudsman to rectify, block, erase or destroy Inaccurate Personal Data and action taken by the Department of Planning to comply with such orders.
h. The Department of Planning shall ensure that appropriate systems are in place to rectify Inaccurate Personal Data or ensure Inaccurate Personal Data can be blocked, erased or destroyed if rectification is not possible or appropriate in the circumstances. See **Data Accuracy** (section 6.9) for more details.

6.6.4 **The right to restrict or stop Processing**: The right to stop or restrict the Department of Planning's use of Personal Data relating to the Data Subject, under certain conditions.

a. All the Department of Planning employees are required to be trained on how to recognise a notice from a Data Subject to stop or restrict Processing of Personal Data.
b. All the Department of Planning employees are required to immediately report notices to stop or restrict Processing of Personal Data to the Data Protection Leader.
c. The Department of Planning shall ensure there are processes in place to respond without undue delay to a notice from a Data Subject who requires that the Department of Planning stop or restrict Processing of their Personal Data in whole, in relation to certain purposes, in certain manners.
d. The Department of Planning shall ensure there are procedures in place to inform Data Subjects if and when The Department of Planning stops or restricts Processing of the Data Subject's Personal Data in response to a notice from the Data Subject.
e. The Department of Planning shall ensure that if a notice to stop or restrict Processing of Personal Data is lawfully denied, the Department of Planning responds to the Data Subject with the reason why it will not comply with the notice. This response will be provided to the Data Subject as soon as practicable and, in any event, within 21 calendar days of receiving the notice in writing.
f. The Department of Planning shall have processes in place to identify and document situations where a Data Subject has applied to the Ombudsman following the failure of the Department of Planning to comply with a notice or request to stop or restrict Processing their Personal Data.
g. The Department of Planning shall ensure the Data Protection Leader maintains an up-to-date log of notices to stop or restrict Processing of Personal Data, where the notices relate to processes within their control.
h. The Department of Planning shall ensure there are processes in place to stop or restrict Processing of Personal Data on its systems without undue delay.
i. The Department of Planning shall ensure there are processes in place to indicate that Processing of Personal Data is restricted on its systems.

6.6.5 **The right to stop direct marketing:** The right that a Data Subject has to cease the use of their Personal Data for direct marketing purposes by the Department of Planning.

a. All the Department of Planning employees are required to be trained on how to recognise a notice to stop direct marketing and understand that the right to stop direct marketing is absolute.
b. All the Department of Planning employees are required to immediately report any notice or purported notice to stop direct marketing to the Data Protection Leader.
c. The Department of Planning shall ensure the Data Protection Leader maintains an up-to-date log of objections to direct marketing, where the direct marketing in question is a process within their control.

d. The Department of Planning shall ensure there are processes in place to ensure that the Department of Planning responds to a notice to stop direct marketing without undue delay.

6.6.6 **Rights in relation to automated decision-making:** At this time, the Department of Planning does not make any decisions based on the automated Processing of Personal Data. The Department of Planning recognises that if it chooses to engage in automated decision-making in the future it must uphold the rights of Data Subjects and will amend this Policy accordingly.

6.6.7 **The right to complain:** Data Subjects have the right to complain to the Ombudsman about any perceived violation of the DPA by the Department of Planning.

a. The Department of Planning shall ensure that there are processes in place to allow complaints to be received and resolved by the Department of Planning before escalation to the Ombudsman. The Data Protection Leader will lead on the response to a complaint from a Data Subject.
b. The Department of Planning shall ensure the Data Protection Leader maintains an up-to-date log of complaints about any perceived violation of the DPA.

6.6.8 **The right to seek compensation:** The right to seek compensation through the Court when a Data Subject suffers damage due to a contravention of the DPA by the Department of Planning.

6.7 Data Subject Access Requests (DSARs)

6.7.1 As part of the day-to-day operations of the Department of Planning, an employee of the Department of Planning may receive SARs from Data Subjects or their representatives seeking to exercise their rights under the DPA. Employees may also receive less formal, including verbal, requests for their Personal Data or information about why and how it is being Processed by the Department of Planning.

6.7.2 The Department of Planning shall ensure all employees know what information, including Personal Data, can be provided to Data Subjects in the normal course of business or under other policies and procedures and when employees must refer a Data Subject or their representative to the Information Manager in accordance with this Policy, including for assistance in formulating a SAR.

6.7.3 All DSARs received by the Department of Planning shall be forwarded immediately to the Information Manager.

6.7.4 The Information Manager will be responsible for handling DSARs in accordance with the DPA. A SAR may also be treated as a Freedom of Information request if appropriate. The Department of Planning shall make reasonable efforts to process DSARs and grant the Data Subjects' requests to access their Personal Data and supplementary information without undue delay and within the timeframe required in the DPA.

6.7.5 The Department of Planning shall ensure that an up-to-date log of DSARs is maintained by the Information Manager.

6.8 Data Accuracy

6.8.1 Through reasonable and appropriate measures (i.e. processes and/or tools), the Department of Planning shall ensure that Personal Data Processed by the Department of Planning, particularly if it is to be used to make any decisions, is accurate, up-to-date and complete when considering the purpose(s) of the Processing.

6.8.2 The Department of Planning shall carefully consider any challenges to the accuracy of Personal Data and implement processes to rectify, block, erase or destroy Inaccurate Personal Data and opinions based on Inaccurate Personal Data without delay, including when ordered to do so by the Ombudsman following a complaint by a Data Subject. See also **Rights in relation to inaccurate data** (section 6.6.3).

6.8.3 If Inaccurate Personal Data have been shared with Third Parties by the Department of Planning and are subsequently rectified, blocked, erased or destroyed, each Third Party shall be contacted and informed of the rectification – unless this proves impossible or involves disproportionate effort.

6.9 Data Retention and Disposal

6.9.1 The Department of Planning shall only retain Personal Data for as long as it is needed and in compliance with the legal obligation to create, manage, maintain and dispose of public records under the National Archive and Public Records Act (2015 Revision) and/or any other applicable legislation or legal obligation.

6.9.2 The Department of Planning's relevant disposal schedules set out minimum retention periods and the Department of Planning will adhere to that policy and those schedules.

6.9.3 The Department of Planning shall securely destroy or erase Personal Data from its systems and physical documents when it is no longer required to accomplish the purpose for which it was collected or to comply with legal obligations, including the obligation to maintain and/or archive public records.

6.9.4 When the Department of Planning securely deletes and destroys Personal Data that are no longer required, the Department of Planning shall make every effort to ensure the same Personal Data maintained by Joint Data Controllers and Data Processors are also securely deleted and destroyed. This requirement does not apply where Joint Data Controllers and Data Processors may need to retain (some or all) Personal Data in order to comply with applicable laws or court orders.

6.9.5 The Department of Planning shall align retention policies and disposal schedules with the DPA, **CIG Privacy Policy** and other relevant policies and frameworks.

6.9.6 The Department of Planning shall either de-identify, anonymise, secure or destroy Personal Data when the Personal Data are no longer required for a specific purpose to mitigate the risk of a Personal Data Breach.

6.10 Data Protection Impact Assessments (DPIAs)

6.10.1 The Department of Planning shall, when introducing new processes, services, programmes or technologies that Process Personal Data, or in the event of a significant change to an existing process, service, programme or technology that Processes Personal Data, assess whether this Processing poses a high risk to the privacy and other rights and freedoms of Data Subjects.

6.10.2 In determining whether Processing of Personal Data poses a high risk to the rights and freedoms of Data Subjects, the Department of Planning shall consider the nature, scope, context and purpose of the Processing.

6.10.3 As part of the risk analysis, the Department of Planning may carry out an assessment of the impact of the planned Processing on the protection of Personal Data using established DPIA procedures.

6.10.4 Where the Department of Planning is drawing up administrative measures or rules relating to the protection of Data Subjects' rights and freedoms with regard to Personal Data Processing, the Department of Planning shall, as required by the DPA, consult the Ombudsman on the content of such measures or rules in accordance with the guidelines issued by the Ombudsman and using the relevant consultation form.

6.11 Sharing Data with Joint Data Controllers, Data Processors and Third Parties

6.11.1 Prior to sharing Personal Data with a Joint Data Controller, sharing Personal Data with a Data Processor, or disclosing Personal Data to a Third Party, the Department of Planning shall ensure that the proposed Processing complies with the Data Protection Principles and other requirements of the DPA, including the requirement to identify a legal basis or legal bases for the Processing. See also **Legal Bases / Conditions of Processing** (section 6.2).

6.11.2 The Department of Planning shall ensure that its Data Processors comply with the Data Protection Principles when Processing Personal Data on behalf of the Department of Planning as the Data Controller.

6.11.3 The Department of Planning shall ensure all parties have sufficient clarity in relation to data protection roles, responsibilities and requirements – including through the establishment of appropriate written contractual or similar measures via an MOU, Terms of Service or Data Processing Agreement – when any of the following situations occur:

a. The Department of Planning or an associated statutory body, as a Data Controller, uses a Data Processor to Process Personal Data;
b. The Department of Planning acting as a Data Processor, engages another Data Processor (i.e. Sub-Processor);
c. The Department of Planning or an associated statutory body and one or more other Data Controllers are identified as Joint Data Controllers; and/or
d. The Department of Planning or an associated statutory body as a Data Controller regularly discloses Personal Data to a Third Party, including another Public Authority.

6.11.4 Where the Department of Planning engages a Data Processor, the terms and conditions of the sharing of Personal Data shall be documented in an MOU (between Public Authorities), in Terms of Service that have been established by the Data Processor (where one Public Authority acts as a Data Processor for two or more other Public Authorities) and agreed by all Data Controllers, or in a Data Processing Agreement (between a Public Authority and a non-CIG Data Processor).

6.11.5 The Department of Planning shall ensure that all Data Processors providing services to the Department of Planning are contractually required to follow the policies set forth herein, or substantially equivalent standards, and to protect Personal Data in accordance with all relevant laws, regulations and rules, and subject to any appropriate security measures and directions from the Department of Planning. These requirements should also apply to any subcontractors that may be engaged by the Data Processor.

6.11.6 Prior to disclosing Personal Data to a Third Party, the Department of Planning shall ensure the proposed disclosure complies with the Data Protection Principles and other requirements of the DPA, including the requirement to identify a legal basis or legal bases for the disclosure.

6.12 International Transfers

Personal Data may be transferred outside of the Cayman Islands to another country or territory only when the receiving country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data. There are limited exceptions to this legal requirement.

6.12.1 The Department of Planning shall refrain from transferring Personal Data to countries or territories that do not have adequate protections for Personal Data. This means that the Department of Planning will only transfer Personal Data to a Person, including a Data Processor, that is located in a country or territory that ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data, unless an exception under Schedule 4 of the DPA applies. See **CIG Privacy Policy Appendix D: International Transfers** for more details.

6.12.2 The Department of Planning shall ensure that measures are in place to ensure that an appropriate MOU (used between Public Authorities) or Data Processing Agreement (used with external suppliers and service providers) is executed with a Data Processor or that appropriate Terms of Service (for Public Authorities that serve as Data Processors for multiple Public Authorities) have been agreed by the Data Controller(s) before Personal Data are transferred internationally to that Data Processor, and that such contracts or other governing documents contain appropriate data protection clauses.

6.12.3 The Department of Planning shall ensure that if Personal Data may be transferred to a Recipient, including a Data Processor, located outside the Cayman Islands, measures are in place to ensure that appropriate international data transfer mechanisms are designed, adopted and implemented prior to the transfer to ensure that Personal Data that are or may be transferred internationally are adequately protected.

6.12.4 Where appropriate, the Department of Planning shall incorporate any standard contractual clauses published and/or approved by the Ombudsman in MOUs, Terms of Service or Data Processing Agreements that include or may require the international transfer of Personal Data.

6.13 Security

6.13.1 The Department of Planning shall Process Personal Data in a manner that maintains confidentiality, integrity and availability, considering the circumstances and risks of the Processing and compliance with relevant local and international legislation and rules as well as contractual obligations. Appropriate physical, technical and organisational security measures shall be taken against unauthorised or unlawful Processing of Personal Data, including to protect Personal Data from accidental loss, destruction or damage.

6.13.2 The Department of Planning shall adopt the **CIG Information Security Policy**.

6.13.3 The Department of Planning uses a range of physical, technical and organisational measures to safeguard Personal Data, including through our Data Processors. These measures include but are not limited to:

a. Developing and maintaining written plans to identify, prevent, detect, respond to, and recover from security threats, events and incidents;
b. Developing robust authentication procedures for accessing all systems that store Personal Data;
c. Administrative and technical controls to restrict access to Personal Data on a "need to know" basis;
d. Maintaining systems, software and applications, anti-virus software, firewalls, and other computer security safeguards, and appointing appropriate personnel to be responsible for keeping such safeguards up to date, including through actions such as patching, licence renewals/expiry monitoring, system health checks and account/user access management;
e. Requiring Data Processors who Process Personal Data on behalf of the Department of Planning to maintain appropriate security measures, including through MOUs, agreed Terms of Service or Data Processing Agreements;
f. Maintaining appropriate records of access to and Processing of Personal Data;
g. Ensuring employees are trained on security policies and measures that have been implemented;
h. Auditing security measures implemented to safeguard Personal Data at regular intervals, including when changes have been made to systems or processes and when legislative changes impact the Processing of Personal Data, and recording the results of such audits;
i. Using appropriate measures, such as encryption, pseudonymisation and chain of custody records, to protect Personal Data, including when stored on laptops, tablets, external hard drives, USB drives and other portable storage devices;
j. Utilising appropriate and secure methods to destroy Personal Data as legally required; and
k. Taking all other reasonable measures as required from time to time by legislation, rules and policies.

6.14 Incident Reporting and Response

6.14.1 The Department of Planning shall ensure that the suspected theft, loss or unavailability of Personal Data, other unauthorised Processing of Personal Data, or damage to Personal Data is immediately investigated.

6.14.2 The Department of Planning shall take steps to immediately examine the cause of a security-related event and make efforts to contain any incidents or breaches and mitigate any risk of harm.

6.14.3 The Department of Planning shall adopt the CIG Information Security Incident Management Policy & Procedure.

6.14.4 The Department of Planning employees shall immediately report any suspected security incidents involving Personal Data to their manager or to the Data Protection Leader.

6.15 Personal Data Breach Notification

6.15.1 The Data Protection Leader shall be notified of any suspected or actual Personal Data Breach in accordance with the CIG Information Security Incident Management Policy & Procedure or in accordance with the MOU/Terms of Service/Data Processing Agreement where the Department of Planning has engaged a Data Processor, is serving as a Data Processor, or is a Joint Data Controller with another Public Authority.

6.15.2 In the event of a security incident involving Personal Data, the Chief Officer/Director of Planning or their designate, shall investigate the incident to determine whether a Personal Data Breach has occurred. All Public Officials and Data Processors shall assist with an investigation if required.

6.15.3 The Director of Planning or his delegate shall be authorised to determine that a Personal Data Breach has occurred and may be advised on this matter by other persons as appropriate, including but not limited to the relevant Data Protection Leader, information security advisors and legal counsel.

6.15.4 The Department of Planning shall assess each Personal Data Breach to determine whether it is likely to prejudice the rights and freedoms of the affected Data Subjects.

6.15.5 The Data Protection Leader shall, under the direction of the Director of Planning, report Personal Data Breaches to the Ombudsman and to impacted Data Subjects in line with the requirements of the DPA. Notifications shall be provided without undue delay and shall describe, at minimum:

a. the nature of the breach;
b. the consequences of the breach;
c. measures taken or proposed to be taken by the Department of Planning to address the breach; and
d. measures recommended by the Department of Planning to the Data Subject to mitigate the possible adverse effects of the breach.

6.15.6 The Data Protection Leader shall maintain a record of all Personal Data Breaches, including:

a. the nature of the breach;
b. likely consequences of the breach for Data Subjects;
c. categories of Data Subjects concerned;
d. types and amount of Personal Data involved;
e. the cause of the incident (if known);
f. how the breach was identified;
g. the date and time the breach occurred (if known);
h. the location and duration of the incident;
i. the date and time the breach was identified;
j. if the breach occurred at a Data Processor, the identity of the Data Processor;
k. remedial actions proposed to be taken to address the breach;
l. remedial actions taken to address the breach;
m. when the breach was reported to the Ombudsman and to affected Data Subjects; and
n. when the case was closed.

6.16 Training and Awareness

6.16.1 The Department of Planning shall ensure that all Department of Planning employees and other Public Officials who handle or have access to Personal Data on its behalf are aware of their responsibilities under this Policy and other relevant data protection and information security policies and procedures.

6.16.2 All employees of the Department of Planning shall receive data protection training at least annually or when there are significant changes to the processes and/or to this Policy. Public Officials who handle or have access to Personal Data, including members of boards and committees, shall receive data protection training as soon as practicable after their appointment or engagement.

6.16.3 The Department of Planning shall ensure that its employees receive and attend the required data protection training, including the content and handling of this Policy and any additional data protection training specific to their role, if they have access to Personal Data.

6.16.4 All Recipients of Personal Data Processed by the Department of Planning shall be made aware of both their individual responsibilities and of the Department of Planning's responsibilities under the DPA and under this Policy.

6.16.5 The Department of Planning shall ensure that all its employees receive and attend training to identify DSARs and other requests or notices where Data Subjects are seeking to exercise other Data Subject Rights, and how to respond or forward the request or notice to the Information Manage. See also **Individual Rights** (section 6.6).

6.17 Acting as a Data Processor

The Department of Planning will be considered a Data Processor when Processing Personal Data on behalf of a Data Controller, which may be a separate Public Authority. In this capacity, the main data protection responsibilities of the Department of Planning acting as a Data Processor are:

6.17.1 Ensuring that an MOU or Data Processing Agreement is in place with the Data Controller(s) or that the Department of Planning has established clear Terms of Service that have been agreed by the Data Controller(s);

6.17.2 Ensuring that all activities and tasks of the Department of Planning are carried out as agreed in the MOU, Terms of Service or Data Processing Agreement;

6.17.3 Maintaining a RoPA or other Personal Data inventory or map if required to do so, including as per the MOU, Terms of Service or Data Processing Agreement.

6.17.4 Implementing appropriate security measures to protect the Personal Data Processed by the Department of Planning on behalf of the Data Controller;

6.17.5 Informing the Data Controller in the event of a Personal Data Breach within the stipulated timeframe outlined in the MOU, Terms of Service or Data Processing Agreement; and

6.17.6 If clearly and solely responsible as per the MOU, Terms of Service or Data Processing Agreement, informing the Ombudsman of Personal Data Breaches within the stipulated timeframe(s), subject to any exemptions that may apply.

6.18 Exemptions

An exemption applies where some or all requirements or rights of the DPA are changed in relation to specific Personal Data Processing. Some exemptions are partial (i.e. allowing the Data Controller or Data Processor to not follow certain provisions, provided certain circumstances exist and/or other provisions are followed). They are generally specific to particular provisions or requirements of the DPA and set out in Part 4 of the DPA (Exemptions). All other provisions of the DPA, outside of the specified exemption, continue to apply.

The Department of Planning will carefully consider the circumstances in which exemptions apply to its Processing activities.

7. DATA PROTECTION LEADER

The Department of Planning has appointed a Data Protection Leader to oversee implementation, enforcement and maintenance of this Policy and to carry out the duties as set out in the **CIG Privacy Policy**.

If you have any questions about this Policy or how Personal Data are handled, or if you need to report an actual or suspected Personal Data Breach, please contact the Data Protection Leader.

Name: Kevon Thompson

Phone Number: (345)244-6501

Email Address: kevon.thompson@gov.ky

Address: The Department of Planning
Cayman Islands Government
PO Box 113
Grand Cayman KY1-9000
Cayman Islands

8. POLICY MONITORING AND COMPLIANCE

Violation of this Policy may result in disciplinary action up to and including termination of employment.

Legal sanctions may also be pursued, if appropriate and as defined by the DPA or other relevant legislation. Unlawfully obtaining or disclosing Personal Data, or procuring the disclosure of Personal Data, is a criminal offence under the DPA.

9. POLICY EVALUATION AND CHANGE

Any employee of the Department of Planning or other Public Official may recommend changes to this Policy through their manager or directly to the Data Protection Leader.

This Policy will be formally reviewed by the Data Protection Leader in consultation with the Director of Planning for its completeness, adequacy, and alignment to the functions and priorities of the Department of Planning at least annually, and on a more frequent basis if deemed necessary. All employees will support the review of this Policy, as required.

All substantive amendments of this Policy will be approved by the Director of Planning.