



Passport & Corporate Services Office
Cayman Islands Government
External Privacy Notice Template

Version: 1.1

Initial release date: 15 February 2022

Date of current version: 17 November 2022

Document Administration

Document location:	CIG intranet ("the Hub") (thehub.gov.ky/task/privacy-policy)
Document name:	Cayman Islands Government External Privacy Notice Template

Revision Record

Version	Date	Revision Description	Author
1.0	15 February 2022	Initial document issued	Information Rights Unit
1.1	17 November 2022	Includes new communications and public relations activities purpose; expands information on recruitment and selection processes; includes sample legal bases for Processing Sensitive Personal Data; expands on or adds various explanatory notes – including in relation to Children’s data, security measures and verifying Personal Data with third parties; additional minor revisions for clarity	Information Rights Unit

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 Hub and can also be obtained by email on request to InformationRights@gov.ky.

Background

The Cayman Islands Data Protection Act (2021 Revision) (“DPA”) introduces what is known as “The Right to be Informed”. This promotes transparency and grants individuals the right to be informed about how their Personal Data are collected, used, or otherwise Processed by Data Controllers. Requirements of the DPA are set out below.

1. The DPA requires, at a minimum, the following information be provided to each Data Subject as soon as reasonably practicable in order to ensure Processing of Personal Data is fair:
 - a. The identity of the Data Controller, i.e. the name of the Public Authority or other Person; and
 - b. The purpose(s) of Processing.
2. In addition, under the DPA, Data Subjects are legally entitled to request and receive from a Data Controller, with limited exemptions, a description and copy of their Personal Data being Processed by the Data Controller as well as the following supplementary information:
 - a. The source(s) of Personal Data being Processed by the Data Controller;
 - b. The Recipients or categories of Recipients to whom the Personal Data may be disclosed;
 - c. The details of any (direct or indirect) transfers outside of the Cayman Islands;
 - d. The general measures taken to keep the Personal Data secure; and
 - e. The details of any automated decision making.
3. Additional information that may be provided to Data Subjects but is not required by the DPA, unless ordered to do so by the Ombudsman, includes:
 - a. The categories of Personal Data Processed by the Data Controller;
 - b. The legal bases of Processing (including statutory requirements/legitimate interests, if applicable);
 - c. The retention period for Personal Data;
 - d. Data Subject Rights and how they may be exercised (except where a request has been received from a Data Subject under section 8 of the DPA, in which case the Data Controller must inform the Data Subject of the right to complain to the Ombudsman under section 43 of the DPA);
 - e. Contact details for the Data Controller’s Data Protection Leader or Data Protection Officer; and
 - f. Changes to the Privacy Notice.

Public Authorities must also be attentive to any other obligations they may have to provide information to Data Subjects – whether proactively or in response to a request – under other legislation, standards or policies.

The Cayman Islands Government (“CIG”) Senior Leadership Team has established a vision statement for the Civil Service to lead privacy and data protection in the Cayman Islands. One of our privacy values is **Transparency: We are open and honest about our processing activities and privacy practices**. While only the identity of the Data Controller and purpose(s) of the Processing must be included in a Privacy Notice and it is a policy decision as to whether more than this is included, this Template includes sections for all of the privacy information listed above. CIG Data Controllers may also choose to first develop a basic Privacy Notice to meet minimum legal requirements of the DPA and then continue to develop the Privacy Notice over time to include more detailed information.

This is a template document and must be read with the CIG Privacy Policy, including to understand all capitalised terms used within guidance notes, including pages i-ii and footnotes throughout. The contents and drafting notes are best practice guidance only and do not constitute legal advice. **A Privacy Notice must be tailored to reflect the specific data collection practices and the purposes of Processing of Personal Data as well as legal requirements around the use of Personal Data.** A Privacy Notice should be reviewed by legal counsel before implementation.

Understanding this Template

Public Authorities may utilise this External Privacy Notice Template (“this Template”) to inform Data Subjects of how their Personal Data will be collected and handled by the Public Authority as a Data Controller. Privacy Notices, or key components of the Privacy Notice (i.e. the identity of the Data Controller and the purpose or purposes of the Processing), should be provided to Data Subjects before collecting any Personal Data. Privacy Notices should be published where any individual can easily access the contents (e.g. on a website, through a link in an email, etc.) and key components should be accessible at all data collection points to meet transparency obligations. Privacy Notices should be provided in writing and may also be adapted for verbal communication at the time of collection.

This Template must be read alongside the DPA, the CIG Privacy Policy, the Data Protection Policy/Policies of the Data Controller using this Template, and any other legislation or policies to which the Data Controller may be subject, including any applicable legislation of the United Kingdom or of the European Union.

When developing a Privacy Notice using this Template, please note it is intended to assist you in creating a “complete” Privacy Notice, detailing all relevant privacy information to external Data Subjects in order to promote transparency of your Processing activities and gain the trust of the people you serve. By publishing information that Data Subjects are entitled to request in writing under the DPA, you may also be able to respond to future Subject Access Requests for “supplementary information” by simply providing a link to your Privacy Notice.

A Privacy Notice aims to provide Data Subjects with clear and concise information about why you are collecting their Personal Data and what you intend to do with it. However, completing this Template and posting a Privacy Notice on your website does not necessarily mean your legal obligations have been met and your Processing activities are transparent. For example, if your premises have CCTV cameras, people who come to your office probably didn’t go online and read your Privacy Notice before entering the building. Therefore, you will need to ensure all visitors are properly notified of your use of CCTV by posting signage at all entrances.

It is generally best to use the same medium you use to collect Personal Data to deliver your privacy information. We have recommended a number of tactics below to effectively communicate privacy information and ensure your Data Subjects receive, at minimum, the key components of your Privacy Notice to ensure Processing is fair. However, **you will need to carefully consider how you interact with your Data Subjects and how you collect Personal Data, which may vary, to determine the most effective way(s) to communicate privacy information.**

Layered Approach: Provide a short statement identifying the Data Controller and the purpose(s) of the Processing (Layer 1), provide a summary of Privacy Notice “highlights” (Layer 2), provide a complete Privacy Notice (Layer 3).

“Just-In-Time” Notifications: Provide key components of the Privacy Notice at the point of collection. Examples:

- When completing a form online that asks for medical information, a notification pops up to tell the Data Subject why this information is being collected, what will be done with it, and what choice is available.
- At a customer service counter or in a call centre, staff are trained to explain what will be done with Personal Data that may be provided by a customer who walks into the office or calls for service.
- An application form explains how the Personal Data that are being requested by the Data Controller will be used and includes a link to the website where the full Privacy Notice can be reviewed by the applicant.

Icons/Symbols: Use familiar icons or symbols to draw attention to data collection or Processing. Examples:

- Hovering over an information symbol on a web form tells you how specific Personal Data will be used.
- A camera image outside of a building shows people there are cameras that may be recording them.

Dashboards: Give Data Subjects greater control of their Personal Data by offering a dashboard allowing them to view and manage Personal Data you have collected from them. This may also reduce the administrative burden of ensuring Personal Data are accurate and up to date, and of responding to requests for information, including SARs.

Privacy Notice¹

1. Scope

The Cayman Islands Government² Passport & Corporate Services Office P&CSO, e.g. “the Department”>,³ respects your privacy and takes care in protecting your personal data. As a data controller, we comply with the Cayman Islands Data Protection Act (2021 Revision) (the “Cayman Islands DPA” or “DPA”). This privacy notice (“Privacy Notice”) demonstrates our commitment to ensuring your personal data is handled responsibly and applies to the “P&CSO”.⁴

2. What Personal Data We Collect

The “P&CSO” collects personal data, including sensitive personal data,⁵ directly from you and may also collect your personal data indirectly from third party sources. Personal data collected by the “P&CSO” is limited to what is necessary for our processing activities. In this Privacy Notice, personal data includes any data relating to an identified or identifiable living individual and includes: name, date of birth, telephone address, email address physical address, parent’s info if relevant to your application.

Personal data we collect directly from you⁶

The “P&CSO” collects the following information directly from you:

- a. Personal data you provide through the “P&CSO” website(s), such as:
 - i. Personal data provided within comments and questions, including your name and/or email address if you provide these details in our web form. If you ask questions about our public services and programmes or provide information about your relationship with us, this may also reveal other personal data, e.g. your employment status, health information, or property ownership;⁷
 - ii. Your email address and subscription preferences if you sign up for our newsletters or notifications, and how you utilise our emails, including whether you open them and which links you click; and
 - iii. Your Internet Protocol (“IP”) address, details of which device or version of web browser you used to access our website content, and other information about how you used our website. .
- b. Personal data you provide when you visit the “P&CSO” offices and other locations, contact us by email or telephone, or access our programmes and services, including our online services⁸;
- c. Personal data that you provide when you inquire about or apply for a job with the “P&CSO”;

¹ Note: Separate templates are available to communicate privacy information to employees and for the use of Cookies on websites.

² Remove “Cayman Islands Government” if this Template is being used by a Statutory Authority or Government Company.

³ Note: The abbreviated term or generic designation is subsequently referred to throughout this Template as [“Data Controller”].

⁴ Recommendation: Include a statement of what is not in scope of this Privacy Notice, as relevant (e.g. employees and prospective employees). If the Data Controller maintains multiple Privacy Notices (e.g. one for external customers and one for internal customers if the Public Authority provides relevant services to other Public Authorities) and/or another Data Controller (e.g. a Board or Committee served by the Public Authority) has related functions and maintains a separate Privacy Notice, include links to these Privacy Notices. If this Privacy Notice will cover multiple Data Controllers, carefully consider how to structure the Privacy Notice to meet legal obligations.

⁵ Remove “, including sensitive personal data,” if the Data Controller does not process *any* sensitive personal data. Please see the definition of “sensitive personal data” in section 3 of the DPA for a list of Personal Data elements that are defined as being sensitive.

⁶ Recommendation: Include a comprehensive list of Personal Data collected directly from the Data Subject and the sources. Examples are listed in this section. Additional examples may include account creation, online forms, registrations and purchases, etc. Do not list a specific example if you do not actually collect that type of Personal Data; entire sections may need to be removed from this Template.

⁷ Recommendation: Review these examples and ensure the types of personal data that may be revealed are relevant and appropriate.

⁸ Remove “, including our online services” if the Data Controller does not provide any services online.

- d. Personal data collected via CCTV at the “P&CSO” premises, including images via cameras located at P&CSO and images with audio via cameras at P&CSO and
- e. Any information you choose to provide when interacting with the “P&CSO” on social media platforms, including facebook.

Personal data collected from other sources⁹

3. How We Use Your Personal Data¹⁰

The purpose of the Civil Service is to make the lives of those we serve better. We are dedicated to supporting the elected government by delivering caring, modern and customer-centred public services and programmes, which deliver value for money.¹¹ The “P&CSO” may use your personal data for the following purposes:

- a. Implementing policies, providing services and programmes, and managing your relationship with us;
- b. Responding to your inquiries;
- c. Verifying your identity;
- d. Measuring how users interact with the “P&CSO”’s website and continually improving our communications channels (including by aggregating personal data collected using cookies);
- e. Communicating and interacting with website visitors;
- f. Sending you marketing communications;¹²
- g. Communications and public relations activities;
- h. Managing accounts payable and receivable, preventing fraud, and protecting public funds;
- i. Statistical and other reporting, both internally and externally;
- j. Seeking legal advice, and exercising or defending legal rights;
- k. Complying with our legal obligations, including all legislation that applies across the public sector;
- l. Communicating and interacting with job applicants and related third parties (e.g. references) and carrying out recruitment and selection processes.¹³

⁹ Recommendation: Include a comprehensive list of Personal Data collected indirectly, i.e. from someone other than the Data Subject, and the sources. Examples may include third parties that verify Personal Data provided by the Data Subject, third parties that share employment and related information (e.g. references, background checks for prospective employees, Personal Data such as CVs that may be provided by third party recruiters), Personal Data collected from publicly available sources (including social media platforms) for any purpose, the purchase of Personal Data for marketing and other purposes, etc. If third parties are explicitly named as providing Personal Data, ensure the Privacy Notice is continuously reviewed to reflect any changes to these third parties.

¹⁰ Include a comprehensive list of how and why the Data Controller may use the Personal Data that is collected. See examples listed.

¹¹ This wording is from the Civil Service purpose statement and mission statement. It must be adjusted if this Template is used by a Statutory Authority or Government Company, i.e. to reflect its own mission statement or otherwise describe its over-arching purpose.

¹² Recommendation: Include information and links advising individuals of how they can opt-out of certain communications, especially if based on Consent, or remove this paragraph entirely if the Data Controller does not engage in direct marketing communications. Note: Communicating with individuals about public services and programmes they are using is not the same as direct marketing. See section 11 of the DPA for a definition of “direct marketing” and to understand a Data Subject’s right to stop processing for this purpose.

¹³ The Data Controller’s Employee Privacy Notice is a separate document that will cover all Processing of Personal Data after the Data Subject signs an Employment Agreement with the Cayman Islands Government. The External Privacy Notice developed using this Template should cover all pre-employment Processing of Personal Data relating to potential job applicants and candidates for specific recruitments. It must consider and reference, as appropriate, the Privacy Notice for the e-recruitment portal CAREERS.GOV.KY: <https://careers.gov.ky/application/custom/English/privacy-statement.html>. If a recruitment process takes place other than through CAREERS.GOV.KY (e.g. for interns or temporary employees), the Data Controller must communicate all relevant privacy information.

4. How We Share Your Personal Data¹⁴

The “P&CSO” may share your personal data as required, including under applicable legislation, with recipients that include joint data controllers, our data processors, and third parties. We will only share your personal data as permitted by the Cayman Islands DPA.

Your personal data may be shared with the following recipients that support our public functions and operations:

- a. **With other public authorities:**¹⁵ Personal data may be shared with other public authorities – here, “public authorities” means Ministries, Portfolios, Offices, Departments, Statutory Authorities, Statutory Bodies and Government Companies – for the purposes set out in this Privacy Notice.¹⁶
- b. **With data processors external to the CIG:** Personal data may be shared with persons providing services to the “P&CSO” as a data processor in compliance with the Cayman Islands DPA. These service providers are only able to use personal data under our instructions and may include:¹⁷
 - i. [Webhosting];
 - ii. [Information Technology];
 - iii. [Records and Information Management, including storage facilities];
 - iv. [Communications];
 - v. [Marketing and campaigns];
 - vi. [Events management]; and
 - vii. [Security operations and fraud prevention].
- c. **With legal advisors and other persons if required by law or in relation to legal proceedings or rights:** Personal data may be disclosed as legally required, for the purpose of or in connection with proceedings under the law, if necessary to obtain legal advice, or if the disclosure is otherwise necessary to establish, exercise or defend legal rights. This may include disclosing your personal data for the following purposes:
 - i. Seeking legal advice;
 - ii. Exercising or defending legal rights;
 - iii. Complying with internal and external audits or investigations by competent authorities;
 - iv. Complying with information security policies or requirements; and

5. Our Legal Bases for Processing Your Personal Data¹⁸

¹⁴ Recommendation: Include a list of third parties’ Personal Data may be shared with and the purpose for sharing.

¹⁵ Note: In every instance where Personal Data are shared with another Public Authority, the Data Controller must establish the legal basis/bases of Processing and ensure the sharing of those Personal Data also complies with all other Data Protection Principles.

¹⁶ Recommendation: If you regularly share Personal Data with one or more other Public Authorities, that/those Public Authority/ies should be named within this section of the Privacy Notice along with the purpose of the sharing. This Privacy Notice may also note whether the relationship is one of Joint Data Controllers, Data Controller to Data Controller, or Data Controller to Data Processor.

¹⁷ Recommendation: Include a comprehensive list of the types of service providers used by the Data Controller and what service they provide. See examples listed. If possible, you may also name your external Data Processors. If Data Processors are explicitly named in this section, ensure the Privacy Notice is continuously reviewed to reflect any changes and consider also listing Data Processors that are other Public Authorities in the section above, e.g. the Computer Services Department as an Information Technology service provider.

¹⁸ Recommendation: Review and ensure the lists of legal bases in this section are comprehensive. Remove any legal bases that will never be relevant to the Data Controller’s Processing activities. As far as possible, include examples of Processing activities undertaken by the Data Controller that will rely on each legal basis where <insert examples> appears. Note: In the DPA, the list of legal bases for Processing Sensitive Personal Data (see Schedule 2) are different than the list of legal bases for all Personal Data (see Schedule 3).

Depending on applicable laws and other circumstances, the “P&CSO” will rely on specific legal bases, or “conditions of processing”, under the Cayman Islands DPA to process your personal data. These may include:

- a. A **legal obligation** to which the “P&CSO” is subject, to: Passport Act (2022 Revision), British Nationality Act (1982), Marriage Act (2010 Revision), Children’s Act (2012 Revision), Adoption of Children Act (2021 Revision) and to comply with various obligations under the Procurement Act, 2016 and Procurement Regulations (2022 Revision), the Public Management and Finance Act (2020 Revision) and Financial Regulations (2022 Revision), the Public Service Management Act (2018 Revision) and Personnel Regulations (2022 Revision), and the National Archive and Public Records Act (2015 Revision);¹⁹
- b. To exercise **public functions**, including the functions of the “P&CSO” to Passport Services: e.g. waivers, passport applications. Corporate Services: Legalisation of documents and Special Marriage Licences;
- c. For the purposes of **legitimate interests** pursued by the “P&CSO” or by a third party or parties to whom the personal data may be disclosed, e.g. when disclosing records containing third party personal data in response to a request submitted under the Freedom of Information Act (2021 Revision).

Where we process your sensitive personal data, we will also meet a second legal basis. These may include:

- a. To exercise our **public functions**;
- b. In relation to **legal proceedings**, including obtaining legal advice and otherwise establishing, exercising or defending legal rights.

6. Children’s Personal Data²⁰

The “P&CSO” collects personal data relating to children under the age of 18 to enable us to deliver public services and programmes and carry out our functions. We may collect children’s personal data for any of the purposes set out in section 3 of this Privacy Notice.²¹

7. Security and International Transfers²²

The “P&CSO” has put in place appropriate technical, physical and organisational measures in order to keep your personal data secure. These safeguards to maintain the confidentiality, integrity and availability of your personal data may include locked copies and restricted access as appropriate²³.

The “P&CSO” will not transfer personal data to countries or territories that do not ensure an adequate level of protection for personal data. We may transfer your personal data outside of the Cayman Islands to:

- a. His Majesty’s Passport Office (HMPO) who prints our British Overseas Territories Passports (BOT). HMPO is located in the United Kingdom and processing complied with GDPR

¹⁹ Recommendation: If this list of legal obligations for your Public Authority is very long, use a bullet point for each legal obligation.

²⁰ Alternative language where the Data Controller does not collect any Personal Data relating to Children under the age of 18/Children under the age of 16, whose Personal Data are typically subject to additional protections: “Unless explicitly stated or implied otherwise, our website and our various public services and programmes are not intended for, or intentionally targeted at, children. We do not knowingly collect or maintain personal data about children under the age of [16/18].”

²¹ Alternatively, the Data Controller may include in this section a list of only services/programmes/activities that involve the Processing of Personal Data relating to Children. This is recommended if most Processing activities in section 3 do not include Children’s data.

²² Recommendation: Include measures taken to protect Personal Data.

²³ Review the Data Controller’s Data Protection Policy for a list of measures the Data Controller has implemented (section 6.14.3). These measures may be summarised here at a level of detail appropriate for a Privacy Notice. In addition to the security measures implemented directly by the Data Controller, you should consider security measures that are implemented by your Data Processors.

We will only transfer your personal data to a country or territory that ensures an adequate level of protection for your rights and freedoms in relation to the processing of your personal data, unless there is a relevant exemption or exception under the Cayman Islands DPA. Exceptions may include your consent or appropriate safeguards.

8. How Long We Keep Your Personal Data

The “P&CSO” may store your personal data for as long as we need it in order to fulfil the purpose(s) for which we collected your personal data, and in line with any applicable laws. This includes the National Archive and Public Records Act (2015 Revision), which governs the creation, maintenance and disposal of all public records. Sometimes, we may anonymise your personal data so that it is no longer associated with you.

9. Cookies²⁴

Cookies, in combination with pixels, local storage objects, and similar devices (collectively, "Cookies" unless otherwise noted), are used to distinguish between visitors to a website.

When you visit [Passport & Corporate Services Office | Portfolio of the Civil Service \(gov.ky\)](#), small files known as Cookies may be stored on your computer, phone, tablet or any other device through your web browser. Information is stored in these text files.

Enabling Cookies may allow for a more tailored browsing experience and is required for certain website functionality. In the majority of cases, a Cookie does not provide us with any of your personal data.²⁵

Please see the website’s Cookie Notice for more information about the use of Cookies.²⁶

10. Your Rights

The “P&CSO” will respect and honour your rights in relation to your personal data and implement measures that allow you to exercise your rights under the DPA and other applicable legislation.

In accordance with the DPA, your rights in relation to your own personal data include:

- a. **The right to be informed and the right of access:** The right to request access to all personal data the “P&CSO” maintains about you as well as supplementary information about why and how we are processing your personal data. This is commonly known as a Subject Access Request and certain supplementary information about our processing is contained within this Privacy Notice.
- b. **Rights in relation to inaccurate data:** The right to request the rectification, blocking, erasure or destruction of any inaccurate personal data the “P&CSO” maintains on you. We will ensure, through all reasonable measures, that your personal data is accurate, complete and, where necessary, up-to-date, especially if it is to be used in a decision-making process.
- c. **The right to stop or restrict Processing:** The right to restrict or stop how the “P&CSO” uses your personal data in certain circumstances.

²⁴ This section of this Template is an adapted summary from the **Cayman Islands Government Cookie Notice Template v1.0**. This section of the Privacy Notice must align with the Public Authority’s Cookie Notice, if one is available. If a separate, more detailed Cookie Notice will not be provided on the website, this section of the Privacy Notice may need to be expanded in order to ensure all relevant information about Personal Data Processing activities using Cookies are covered. If the Data Controller does not use Cookies to collect any Personal Data on any website(s), this section may be deleted entirely from the Privacy Notice.

²⁵ Recommendation: Delete this sentence if most Cookies used on the website do, in fact, collect Personal Data.

²⁶ Recommendation: Include a link to the Cookie Notice. If the Data Controller maintains more than one website, include all links. A Cookie Notice is not mandatory and the Data Controller’s External Privacy Notice may be used as an alternative method of providing privacy information to website visitors regarding the use of cookies to Process their Personal Data. If this is done, the External Privacy Notice must include, at minimum, the purpose of all cookies that Process any Personal Data, including the visitor’s IP address.

- d. **Rights in relation to automated decision making:** The right to obtain information about and object to the use of automated decision making by the “P&CSO” using your personal data. The “P&CSO” does not currently use automated means to make decisions about you. However, we will update this Privacy Notice and we will also notify you in writing as required if this position changes.²⁷
- e. **The right to complain:** The right to complain to the Ombudsman about any perceived violation of the DPA by the “P&CSO”.
- f. **The right to seek compensation:** The right to seek compensation in the Court if you suffer damage due to a contravention of the DPA by the “P&CSO”.

You may contact the “P&CSO”, using the contact details listed below, to access and review your personal data or to exercise any other rights provided to you under the DPA. The “P&CSO” will take into consideration circumstances where, under the DPA or other applicable legislation, your rights may be limited or subject to conditions, exemptions or exceptions.

Upon contacting the “P&CSO”, we may need to verify your identity prior to fulfilling a request and may request additional information as required. In accordance with the DPA, the “P&CSO” may also charge a reasonable fee in relation to your request if it is unfounded or excessive in nature, or the “P&CSO” may reserve the right not to comply with the request at all.

To learn more about your rights, visit www.ombudsman.ky.

11. Data Protection Principles

When processing your personal data, the “P&CSO” will comply with the eight Data Protection Principles defined within the Cayman Islands DPA:

- a. **Fair and lawful processing:** Personal data shall be processed fairly. In addition, personal data may be processed only if certain conditions are met, for example the data controller is subject to a legal obligation that requires the processing or the processing is necessary for exercise of public functions.
- b. **Purpose limitation:** Personal data shall be obtained only for one or more specified, explicit and legitimate purposes, and not processed further in any manner incompatible with that purpose or those purposes.
- c. **Data minimisation:** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.
- d. **Data accuracy:** Personal data shall be accurate and, where necessary, kept up-to-date.
- e. **Storage limitation:** Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- f. **Respect for the individual’s rights:** Personal data shall be processed in accordance with the rights of data subjects under the DPA, including subject access.
- g. **Security – confidentiality, integrity and availability:** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- h. **International transfers:** Personal data shall not be transferred to a country or territory unless that 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.

²⁷ Automated decision-making as provided for in the DPA is not common among CIG Data Controllers. If the Data Controller does not engage in automated decision making, you may include this statement in your Privacy Notice. Otherwise, it must be removed.

12. How to Contact Us

The “P&CSO” has appointed a Data Protection Leader.²⁸ If you have any questions about this Privacy Notice or how your personal data is handled, or if you wish to make a complaint, please contact:²⁹

Name: Patricia Stoll, Data Protection Leader

Telephone number: 345-649-2273

Email Address: Patricia.stoll@gov.ky

Address: 128 Sussex House Elgin Avenue, Grand Cayman

The P&CSO aims to resolve inquiries and complaints in a respectful and timely manner.

13. Changes to this Privacy Notice³⁰

The “P&CSO” reserves the right to update this Privacy Notice at any time and will publish a new Privacy Notice when we make any substantial updates. From time to time, the “P&CSO” may also notify you about the processing of your personal data in other ways, including by email or through our publications.

This Privacy Notice was last updated on 21 November 2023.

²⁸ Note: All Civil Service Data Controllers are required to appoint a Data Protection Leader in accordance with the CIG Privacy Policy.

²⁹ Recommendation: Provide the name and contact details for the Data Protection Leader here unless questions and complaints will be directed through another contact, e.g. a general privacy office, the dedicated communications unit, or some other relevant person.

³⁰ Note: The Data Controller must consider if and how changes to the Privacy Notice will be communicated directly to Data Subjects. Where the identity of the Data Controller and/or purpose(s) of the Processing change, Data Subjects must be provided with this new or updated information in order for the Processing of the Personal Data to be considered fair under the First Data Protection Principle.