DATA PROTECTION POLICY

Effective: October 2021

To be reviewed: October 2024

To help the public service
spend wisely

TABLE OF CONTENTS

Data Protection 1

Aim of the Data Protection Policy 1

Purpose 1

Scope 2

National and European Data Protection Laws 2

Rules for Processing and Storing Data 2

Restrictions and Confidentiality 4

Departmental Data Processing 5

Controlling and Updating Data Protection Framework 5

Appendix – CIG Data Protection Regulations 2018 6

DATA PROTECTION

AIM OF THE DATA PROTECTION POLICY

This policy is to provide guidance to Office of the Auditor General (OAG) staff on how to process data received while conducting audits, specifically in relation to the collection and processing of personal data. It is govern by the legislation, policy, standards and information released by the Cayman Islands Government relating to Privacy and Data Protection.

WHAT IS PERSONAL DATA

"Personal data" as describe in the Data Protection Act means data relating to a living individual who can be identified and includes data such as —

(a) the living individual's location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;

(b) an expression of opinion about the living individual; or

(c) any indication of the intentions of the data controller or any other person in respect of the living individual;

PURPOSE

The OAG Data Protection Policy (DPP) aims to act as supplementary to CIG DATA PROTECTION ACT, 2017 DPLaw2017.pdf and Data Protection Act 2021 Revision Data-Protection-Act-2021-Revision.pdf which was enacted in 2017 and brought into force on 30 September 2019; where there are unique or different policy items that apply to the OAG, they are noted in this document and will supersede the CIG Policy. Where there is no conflict with the CIG Data Protection Regulation it will be applied fully by OAG.

In addition to the Act, there is CIG Data Protection Regulation 2018 (appendix I) an additional supplement any document outlining the scope in which the Act should operate and the approved exemptions permitted under the law.

Client personal data in the context related to the Office of the Auditor General relates to the collection of payroll data or any information that is deemed personal in nature.

SCOPE

The DPP applies to all OAG staff and other stakeholders that are permitted to access, process and store personal data related to the OAG's conduct of business. Other Stakeholders being contracted external Auditors employed to by The Office of the Auditor General to conduct Audits on any contracted government agency or Statutory Authority.

The Policy is applicable to all OAG staff (full-time and part-time employees), consultants, students or interns and remote users who are authorised to process and store data on behalf of the OAG (including connecting to our locally hosted servers or accessing remotely from other jurisdictions around the world). Additionally, the rules and regulations in this policy apply to any local and overseas private companies who may provide IT services to the OAG.

However, in accordance with the Constitution Order 2009 provided additional authority to AG under section 114 subsection (4) to the collection of data which states **"The Auditor General, and any person authorised by him or her to act on his or her behalf, shall have access to all books, records, reports and other documents relating to the accounts referred to in subsection (3)."**

DATA PROTECTION COMPLIANCE

The DPP is compliant with the Cayman Islands Data Protection Act that was passed on 27th March 2017 and came into effect on 30th September 2019. It is important to note that this Act takes precedence over DPP in relation to governing data that is developed and processed in Grand Cayman, Cayman Brac and Little Cayman.

The Office of the Ombudsman provides additional support and is the reporting authority in the event a breach occurs. Additional information can be sought and reports can be made by visiting there website https://ombudsman.ky/data-protection

RULES FOR PROCESSING AND STORING DATA

In addition to the requirements outlined in the CIG Data Protection Act, the OAG will adhere to the following data processing and storage rules:

CLIENT DATA

Personal Data is defined as “Information relating to a living person who can be identified”, also noting that some information are also defined as “sensitive personal data” which is subjected to additional protections.

All personal data is to be treated as confidential and will not be shared with any person or persons not directly involved in the OAG business activity associated to the data being processed unless legally permitted. In the event an investigation has been launch, information will be shared with other investigating bodies.

Any requests for access to the data must be authorised in writing or electronic format, as appropriate for the data request, by:

- The OAG Data Protection Officer – pertaining to all external requests for data access; or
- The Auditor General – pertaining to all internal requests for data access by non-aligned personnel, or for FOI issues escalated from the FOI officer.

Data will only be transferred into or out of the OAG’s systems using secure data transfer mechanisms to ensure data security and integrity. Electronic Mail (email) use for data transfer is not recommended unless other, more secure options are not available. If email is used for data transfer, the sender should ensure encryption is available for the data as part of the email software, or must ensure secure encryption using an alternative approach (e.g. encrypted/password protected zip file).

DATA STORAGE

Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Security is about integrity and availability as well as confidentiality, and it is also more than technical solutions. Information security includes appropriate policies and procedures, minimising access to only those individuals with a “need to know”, and training all staff in how to properly handle personal data. Personal data must be kept secure not just from malicious attacks, but also from inadvertent harm.

The OAG will comply with all legally established requirements for the storage and destruction of data.

The OAG will perform a review, archive, and purge process at least once a year. This shall include:

- Archiving Files
  - Files not accessed in the preceding 24 months will be archived using appropriate archiving tools.
  - Archived files will be noted in a tracking system for later review and removal at the appropriate time.
- Purging Files
  - Files which have reached or exceeded the legally established end of life, or a period of seven (7) years where a period is not legally established, will be flagged for purging.
  - All files to be purged will be properly flagged or segregated for review by a senior member of OAG staff.
  - All files to be purged will be properly noted and all required paperwork will be completed and processed with the appropriate CIG authorities to ensure compliance with CIG data policies and with Cayman Islands law.
- Data Duplication
  - The OAG will make every practicable effort to prevent the duplication of data in the file systems.
  - For any client case being performed in an ongoing/periodic fashion, where data from a previous project may be required for use in the current client project, the data should be either:
    - Brought forward to the current case with a referring note placed in the older case; or
    - A note should be placed in the current case, referring to the file located in the older case.

  NOTE: For case management purposes the first option is recommended where possible.

RESTRICTIONS AND CONFIDENTIALITY

OAG will ensure appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. It is pertinent that personal data do not leave the Cayman Islands unless the destination offers a level of protection that is broadly the same or where adequate safeguards are in place to protect the information. This prevents data from being transferred abroad with the goal of avoiding obligations under the Data Protection Act or the unintended consequence of data not being protected to the same level it would be in the Cayman Islands

Security is about integrity and availability as well as confidentiality, and it is also more than technical solutions. Information security includes appropriate policies and procedures, minimising access to only those individuals with a "need to know", and training all staff in how to properly handle personal data. Personal data will be kept secure not just from malicious attacks, but also from inadvertent harm.

Disclosing data to an overseas organisation, using a contractor located outside of the Cayman Islands, and storing data in the "the cloud" will often mean transferring the data overseas. It's important for data controllers to always know where personal data is being stored or transferred and whether it is adequately protected in that jurisdiction.

DEPARTMENTAL DATA PROCESSING

All processing of personal data must take into account the rights of individual data subjects. This is a reminder that we have an obligations towards the individuals whose personal data we process in order to make lives better.

Individual rights under the Data Protection Act include a fundamental right of access to your own personal data and certain supplementary information, the right to restrict or stop processing under certain conditions, the right to know whether decisions are being made through automated means and to request reconsideration, the right to have inaccurate data corrected or erased, and the right to complain and seek compensation for breaches of the Act.

Purpose limitation means that an entity may not collect personal data for one purpose and then use it for another, incompatible purpose.

If a data controller wants to use personal data for a new purpose, they must ensure they have an appropriate legal basis or bases and that the new processing is also fair, i.e. the data subject is made aware of the new purpose as soon as reasonably practicable.

CONTROLLING AND UPDATING DATA PROTECTION FRAMEWORK

All control and updating of the Data Protection Framework is subjected to legislation with the support of Cabinet Office.

Appendix i

CIG DATA PROTECTION REGULATIONS 2018

CAYMAN ISLANDS

Data Protection Law, 2017 (Law 33 of 2017)

THE DATA PROTECTION REGULATIONS, 2018

Arrangement of Regulations

Regulation		Page
1.	Citation	5
2.	Definitions	5
3.	Fees for requests	5
4.	Extension of time for response	6
5.	Data controller's duty to inform data subject of right to complain	6
6.	Circumstances when data controller not obliged to comply	6
7.	Health exemption	6
8.	Education exemption	7
9.	Social work exemption	7
10.	Exceptions to the Eighth principle - international co-operation between intelligence and regulatory agencies	8

CAYMAN ISLANDS

Data Protection Law, 2017 (Law 33 of 2017)

DATA PROTECTION REGULATIONS, 2018

The Cabinet, in exercise of the powers conferred by section 61 of the Data Protection Law, 2017, makes the following Regulations —

Citation

1. (1) These Regulations may be cited as the Data Protection Regulations, 2018.

(2) These Regulations come into force immediately after the *Data Protection Law, 2017* comes into force.

Definitions

2. In these Regulations, —

"child" means a person under the age of eighteen years;

"educational record" means a record of information that —

(a) is processed by or on behalf of the proprietor or a teacher at a school;

(b) relates to a person who is or has been a pupil at the school; and

(c) originated from or was supplied by or on behalf of any of the following persons —

(i) a teacher or other employee at the school;

(ii) a person who is engaged by the proprietor of the school under a contract for the provision of educational services;

(iii) the pupil to whom the record relates; or

(iv) a parent of that pupil; and

"parent" in relation to a pupil, includes a guardian and any person who has custody of the pupil.

Fees for requests

3. (1) Personal data and information pursuant to a request under section 8 shall be provided

free of charge, except that where the request from a data subject is determined to be manifestly unfounded or excessive because the request —

(a) is repetitive;

(b) is fraudulent in nature; or

(c) would divert the resources of the data controller unreasonably, the data controller may charge such fee as covers the cost of providing the requested data and information or may refuse to act on the request and provide the reasons for doing so.

(2) The burden of proving that the request was "manifestly unfounded" or "excessive" is on the data controller.

(3) Where personal data are —

(a) open to access by the public pursuant to any other enactment as part of a public register or otherwise; or

(b) available for purchase by the public in accordance with administrative procedures established for that purpose, access to that data shall be obtained in accordance with the provisions of that enactment or those administrative procedures.

(4) Where a data controller charges a fee pursuant to paragraph (1), the fee shall be reasonable taking into account the administrative cost of providing the personal data or information requested.

Extension of time for response

4. (1) A data controller may extend the time for responding to a subject access request under section 8 by up to thirty days where one or more of the following conditions apply —

(a) a large amount of data is requested or is required to be searched and meeting the timelines would unreasonably interfere with the operations of the data controller;

(b) more time is required to consult with a third party or other data controller before the data controller is able to decide whether or not to give the data subject access to the requested data; or

(c) the data subject has given consent to the extension.

(2) With the permission of the Ombudsman, the data controller may extend the time for responding to a subject access request under section 8 —

(a) for a period longer than thirty days, where one or more of the circumstances described in paragraphs (1)(a) to (c) apply; and

(b) where the Ombudsman otherwise considers that it is appropriate to do so.

(3) Where the time for responding to a request is extended under this regulation, the data controller shall inform the data subject of the reason for the extension and when a final response will be given.

Data controller's duty to inform data subject of right to complain

5. Where a request under section 8 is received from a data subject, the data controller shall inform the data subject of the right to complain to the Ombudsman under section 43 of the Law.

Circumstances when data controller not obliged to comply

6. (1) Without limiting sections 10(2)(a) to (c) of the Law, a data controller shall comply with a request under section 10(1) unless the data controller has applied to the Ombudsman within twenty-one days of the date of the request by the data subject and has received approval from the Ombudsman to not comply with the data subject's request to cease processing.

(2) The data controller shall inform the data subject of any application made to the Ombudsman under paragraph (1).

Health exemption

7. (1) Personal data, the release of which could reasonably cause mental or physical harm to the data subject or any other person, shall be exempt from the subject information provisions.

(2) A data controller who is not a health professional shall not, on the ground of the exemption under paragraph (1), refuse a request for information under this regulation unless —

(a) after receiving the request, the data controller consults the appropriate health professional on the question of whether the exemption applies and obtains in writing from the health professional an opinion that the exemption applies to the information; or

(b) the following conditions are satisfied —

(i) the data controller consulted a health professional before receiving the request;

(ii) the health professional was the person who would have been the appropriate health professional, if the data controller had carried out the consultation under subparagraph (a); and

(iii) the data controller obtained from the health professional an opinion in writing that the exemption applied to all of the information.

(3) The conditions referred to in paragraph (2) are not satisfied if —

(a) the opinion was obtained before the start of the period of six months that ends on the day that the request is made; or

(b) the opinion was obtained within the period in paragraph (a) but it is reasonable in all the circumstances to consult the appropriate health professional again.

Education exemption

8. (1) Personal data that consist of information that constitutes an educational record are exempt from section 8 of the Law to the extent that the application of that section would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

(2) Where a parent, or someone who has been appointed by the court to manage the affairs of a person who is the data subject, is enabled to make a request under section 8 of the Law on behalf of a data subject and has made such a request, personal data that consist of information specified in paragraph (3) are exempt from the provisions in section 8 of the Law to the extent that the application of that section would not be in the interests of the data subject.

(3) For the purposes of paragraph (2), the personal data are data consisting of information

constituting an educational record or information about whether the data subject, where the subject is a child, is or has been the subject of abuse or may be at risk of it.

(4) Personal data that may reveal a record of a question that is reasonably expected to be used on an examination or test within twelve months from the date of the request are exempt from the provisions under section 8.

(5) For the purposes of this regulation, "abuse" in respect of a person when that person is a child —

(a) includes physical injury to and physical neglect, emotional neglect, ill-treatment and sexual abuse of the person; and

(b) excludes accidental injury.

Social work exemption

9. (1) The personal data specified in paragraph (5) are exempt from the subject information provisions to the extent that the application of those provisions would be likely to prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental health or condition of the data subject or any other person would be likely.

(2) In a case where a defined person is enabled by or under any enactment or rule of law to make a request under section 8 of the Law on behalf of a data subject and has made such a request, personal data specified in paragraphs (5)(a) or (b) are exempt from the provisions under section 8 of the Law to the extent that the application of that section would result in the disclosure of information —

(a) provided by the data subject in the expectation that it would not be disclosed to the person making the request;

(b) obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed; or

(c) that the data subject has expressly indicated should not be so disclosed.

(3) Paragraphs (2)(a) and (b) do not apply to the extent that the data subject has expressly indicated that the data subject no longer has the expectation that the information would not be disclosed.

(4) For the purposes of paragraph (2), a "defined person" is a person who —

(a) has parental responsibility for a child who is the data subject; or

(b) has been appointed by a court to manage the affairs of a person who is the data subject and incapable of managing his or her own affairs.

(5) The personal data referred to in paragraph (1) are —

(a) personal data processed by a public authority in relation to any of the following matters —

(i) the allocation of housing or other residential accommodation;

(ii) the provision of any benefit under the *Health Insurance Law* (*2018 Revision*) or the *Poor Persons (Relief) Law* (*1997 Revision*);

(iii) probation;

(iv) school attendance;

(v) ensuring that children receive suitable education whether by attendance at school or otherwise;

(vi) guardianship under the *Grand Court Law* (*2015 Revision*); or

(vii) any function under the *Children Law* (*2012 Revision*), Adoption of Children Law (*2003 Revision*), Mental Health Law, 2013, the *Older Persons Law, 2017* or any other applicable law; or

(b) personal data processed by a court and consisting of information that —

(i) is supplied in a report to or other evidence given to the court in the course of proceedings relating to families or children; and

(ii) the court directs should be withheld from the data subject on the ground that it appears —

(A) to be impracticable to disclose the report or other evidence having regard to the data subject's age and understanding; or

(B) to be undesirable to disclose the report or other evidence having regard to the serious harm that might be suffered by the data subject by the disclosure.

(6) For the purposes of this regulation, "proceedings relating to families or children" includes proceedings relating to adoption, matrimonial matters or guardianship.

Exceptions to the Eighth principle - international co-operation between intelligence and regulatory agencies

10. A transfer for the purposes of international cooperation between intelligence or regulatory agencies as set out in paragraph 10 of Schedule 4 of the Law is limited to a disclosure that is permitted or required under an enactment in force in the Islands or an order issued by the Grand Court.