DATA PROTECTION ACT 2023

Summary of Main Requirements
Assented to on 16 August 2023

Jack A. Alli, Sons & Co. JAS

Table of Contents

Purpose of Legislation

To regulate the collection, keeping, processing, use and dissemination of personal data; to protect the privacy of individuals in relation to their personal data; and to provide for related matters.

Scope

The Act applies to:

a. the processing of personal data in the context of the activities of a data controller or a data processor established in Guyana;
b. the processing of personal data of data subjects in Guyana by a data controller or a data processor not established in Guyana, where
    i. the data controller or data processor uses equipment in Guyana for processing the personal data (other than for transit through Guyana); or
    ii. the processing activities are related to the offering of goods or services to data subjects in Guyana; or the monitoring of the behaviour of data subjects as far as their behaviour takes place within Guyana.

It envisages the establishment of the Data Protection Office which shall be responsible for the administration and implementation of the Act. The President of Guyana shall appoint a Data Protection Commissioner who shall be a person of eminence in public life with wide knowledge and experience in law, science and technology, management or administration and governance.

Roles

The data **subject** means an individual who is the subject of personal data.

The data **controller** means

a. a natural or legal person, public authority, agency or other body who alone, jointly or in common with others determined the purposes for which, and the manner in which, any personal data is or should be processed; or
b. where personal data is processed only for the purposes for which the data is required by or under any law to be processed, the natural or legal person on whom the obligation to process the data is imposed by or under any law.

The data **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Data

Personal data refers to any information relating to an identified or identifiable natural person.
Sensitive personal data means personal data consisting of information on a data subject's:

a. racial or ethnic origin
b. political opinions
c. religious beliefs or other beliefs of a similar nature
d. membership of a political body

e. membership of a trade union
f. genetic data
g. biometric data
h. sexual orientation or sexual life
i. financial record or position
j. criminal record
k. health record
l. proceedings of any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings.

Data Protection Principles

Personal data shall 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 the personal data is processed;
d. accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified, without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
f. 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.

In relation to the fair processing of information, it is necessary that in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has readily available to him or her, the following information:

a. identity of the data controller;
b. where the data controller has nominated a representative, the identity of that representative;
c. identity of the data protection officer;
d. purpose or purposes for which data is intended to be processed;
e. identity of any third party to which disclosure of the personal data is contemplated;
f. legal authority for seeking the personal data, where applicable;
g. whether the provision, by the data subject, of the personal data sought is compulsory under any law, and the consequences of not providing the personal data;
h. expected retention period of the personal data;
i. further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair.

Processing of data shall be lawful where:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; or
b. the processing is necessary for the following, inter alia:
    i. Performance of a contract to which the data subject is a party, or the taking of steps at the data subject's request towards the entering of a contract;
    ii. Compliance with a legal obligation imposed on the data controller (other than a contractual obligation);
    iii. To protect the vital interests of the data subject;
    iv. The administration of justice;
    v. The exercise of any function of Parliament or public authority.

The data controller is required to demonstrate the consent from the data subject, where it is relied upon to process personal data.

Data Controller

Data collectors are required to be registered with in the Register of Data Controllers. A data collector who is not established in Guyana shall nominate a representative established in Guyana, for purposes of the Act.

The data collector shall implement appropriate technical and organisational measures, including measures such as:

» identifying reasonably foreseeable internal and external risks to personal data under the person's possession or control;
» establishing and maintaining appropriate safeguards against identified risks;
» the pseudonymisation and encryption of personal data;
» the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
» verifying that the safeguards are effectively implemented; and
» ensuring that the safeguards are continually updated in response to new risks and deficiencies.

The data controller shall also implement appropriate technical and organisational measures for ensuring that only personal data which is necessary for each specific purpose is processed.

A data controller shall maintain a record of processing activities under his/ her/its responsibility containing the following:

a. the name and contact details of the data controller and, where applicable, the joint data controller, the data controller's representative, and the data protection office;
b. the purpose of the processing;
c. a description of the categories of data subjects and of the categories of personal data;
d. the categories of recipients to whom the personal data has been or will be disclosed including recipients in other countries or international organisations;

e. where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and documentation of suitable safeguards for certain transfers;
f. where possible, the envisaged time limits for erasure of the different categories of data; and
g. where possible, a general description of the technical and organisational security measures.

Data Processor

Data processors are required to be registered with in the Register of Data Processors. A data processor who is not established in Guyana shall nominate a representative established in Guyana, for purposes of the Act.

A data controller may use a data processor only where the data processor implements appropriate technical and organisational measures to ensure the processing will be in accordance with the requirements of the Act and also ensure the protection of the rights of the data subject. Processing by a data processor shall be governed by a written contract between the data processor and data controller which sets out the following (inter alia):

a. the subject-matter and duration of the processing
b. the nature and purpose of the processing
c. the type of personal data and categories or data subjects; and
d. the obligations and rights of the data controller

A data processor shall maintain a record of all categories of processing activities carried out on behalf of a data controller, which contains:

a. the name and contact details of the data processor, data controller(s), representatives (where applicable) and the data protection officer;
b. the categories of processing carried out on behalf of each data controller;
c. where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and documentation of suitable safeguards for certain transfers;
d. where possible, a general description of the technical and organisational security measures.

Data Protection Officer

The data controller and data processor shall designate a data protection officer in any case where:

a. the processing is carried out by a public authority or body, except for a court of competent jurisdiction acting in their judicial capacity;
b. the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope and their purpose, require regular and systematic monitoring of data subjects on a large scale; or
c. the core activities of the data controller or data processor consist of processing on a large scale of sensitive personal data.

A data protection officer shall report directly to highest management level of a data controller or data processor. Among the functions required, a data protection officer will:

a. inform and advise the data controller or data processor and the employees who carry out processing of their obligations under the Act;
b. monitor compliance with the Act and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c. provide advice where requested as regard the data protection impact assessment and monitor its performance.
d. cooperate with the Data Protection Commissioner.

Security Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Consideration must be taken of risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Where there is a breach of personal data, the data controller shall without undue delay and not later than seventy-two hours after having become aware of it, notify the Data Protection Commissioner of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of any person. A data processor shall notify the data controller without undue delay of a personal data breach.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of persons, the data controller shall communicate the personal data breach to the data subject without undue delay and where feasible, not later than seventy-two hours after having become aware of it.

Rights of a Data Subject

A data subject shall have the right to be informed by the data controller whether personal data of that data subject is being processed by or on behalf of the data controller.

Where personal data of the data subject is being processed by or on behalf of the data controller, the data subject has the right to receive the following from the data controller:

a. purpose of the processing;
b. categories of personal data concerned;
c. recipients or categories of recipients;
d. where possible, the envisaged period for which the personal data will be stored;
e. right to request rectification or erasure of personal data;
f. right to lodge compliant with the Data Protection Commissioner;
g. source of available information where personal data not collected rom the data subject.

The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him or her without undue delay.
The data subject shall have the right to obtain from the data controller restriction of processing of personal data where one of the following applies:

a. accuracy of personal data is being contested by the data subject, for a period that allows the data controller to verify the details;
b. the processing is unlawful;
c. personal data no longer required but being retained for legal defence of the data subject;
d. data subject has objected to processing.

The data subject shall have the right to object in writing at any time to the processing of personal data concerning him or her unless the data controller demonstrates compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or the establishment, exercise or defence of a legal claim.

Transfer of Personal Data Outside of Guyana

Personal data shall not be transferred to a country or territory outside Guyana or an international organisation unless that country, territory or international organisation provides for:

a. an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and
b. appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.

Appropriate safeguards may include:

a. a legally binding and enforceable instrument between public authorities;
b. binding corporate rules, as outlined in the Act;
c. standard data protection clauses prescribed by the Commissioner with the approval of the Minister;
d. contractual clauses authorised by the Commissioner between the data controller or data processor and the data controller, data processor or the recipient of the personal data; or
e. provisions, authorised by the Commissioner, to be inserted into administrative arrangements between public authorities which include enforceable and effective data subject rights.

Binding corporate rules mean personal data protection policies which are adhered to by a data controller or data processor for transfers or a set of transfers of personal data to a data controller or a data processor in one or more countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
These requirements do not apply in the following circumstances:

a. the data subject has given his or her consent to the transfer of personal data;
b. the transfer of personal data is necessary for:
    i. the performance of a contract between the data subject and the data controller, or the taking of steps to enter such a contract directly with the data subject or with a party requested by the data subject;
    ii. reasons of substantial public interest;
    iii. in connection with any legal proceedings; or for obtaining legal advice; or establishing, exercising or defending legal rights;
    iv. protection of the vital interests of the data subject.

Data Protection Impact Assessment

Where a type of processing, for instance using new technologies and taking account of nature, scope, context and purpose of processing, is likely to result in a high risk to the rights and freedoms of a person, the data controller shall prior to processing, carry out an assessment of the impact of anticipated processing operations on the protection of personal data.

Exemptions

Certain transfers of personal data are exempt from the disclosure requirements of the Act, including processing of personal data for:

» prevention or detection of crime
» apprehension or prosecution of offenders
» assessment or collection of any tax, duty or other imposition of a similar nature

The Minister may, by order, exempt from disclosure to data subject requirements, or modify those requirements in relation to, personal data:

a. consisting of information as to the physical or mental health or condition of a data subject;
b. in respect of which the data controller is an educational institution and which consist of information relating to persons who are or have been pupils at the educational institution.
c. in respect of which the data controller is a tertiary institution and which consist of information relating to persons who are or have been students at the tertiary institutions.
d. such other information, specified by Order, processed by public authorities, charities or in the course of carrying out social work.

Code of Practice for Data Sharing

The Data Protection Commissioner may prepare and submit to the Minister a data sharing code of practice which contains practical guidance in relation to the sharing of personal data in accordance

with the Act and such other guidance as the Commissioner considers appropriate. Once approved by the Minister, the code of practice comes into operation upon publication in the Official Gazette.

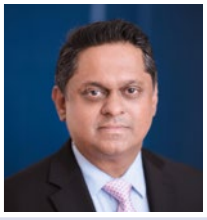
Certification

The Data Protection Commissioner may lay down technical standards for data protection certification mechanisms and data protection seals and marks. Such certification shall be voluntary, issued for a maximum period of three years and withdrawn where requirements are no longer met.

Regulations

Regulations under the Act may address the following (inter alia):

a. provide for additional safeguards in relation to sensitive personal data, including the processing of national identification numbers, national health identification numbers or any other identifier of general application;
b. provide for processing of employee's personal data;
c. provide for the obligation of professional secrecy;
d. prescribe retention periods for personal data to be observed by data controllers;
e. prescribe methods by which personal data may be disposed;
f. prescribe fees.



Author

Khalil Alli
Partner
Jack A. Alli, Sons & Co.
145 Crown Street, Queenstown,
Georgetown, Guyana
592-226-2904
www.jackalli.com
khalil.alli@jackalli.com

Author's Note
The information contained in this article is for general guidance on matters of interest only and is not meant to be comprehensive. It is recommended that you obtain advice specific to your circumstances from professional advisors.