CIDP MAURITIUS

DATA PRIVACY POLICY

Written by	Boboc & Associates (updated and reviewed for local requirements by Rajini Naidoo Cartier, DPO Mauritius)
Approved by	Claire Blazy Jauzac 8/05/2019

1. INTRODUCTION

1.1.Purpose

CIDP Mauritius (CIDP Ltée) takes its responsibilities concerning the requirements of the General Data Protection Regulation (referred to as GDPR) and the Mauritian Data Protection Act (referred to as MDPA) very seriously. The provisions of the present Policy are applicable to all employees, contractors, or any other person, partner of the CIDP, who is processing Personal Data on behalf of CIDP.

1. Definitions

Personal Data means any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person;

Personal Data Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

CIDP means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the CIDP.

Data Protection Authority means an authority which is established in a Member State to be responsible for monitoring the application of GDPR.

Data protection by default means that appropriate security measures must be implemented for the protection of Personal Data processed and stored by existing ICT software/applications/other resources.

Data protection by design means that appropriate security measures must be considered and implemented when developing ICT software/applications/other resources aimed at processing Personal Data.

Data Subject means any natural person (e.g. employees, clients), including individual undertakings and self-employed persons.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of/ access to, Personal Data transmitted, stored or otherwise processed.

Special categories of Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person sex life or sexual orientation.

2. GENERAL PRINCIPLES

2.1. Principles for processing

While carrying out personal data processing activities/operations, CIDP has to comply with the following principles:

(1) *Lawfulness, fairness and transparency* - Personal Data must be processed lawfully, fairly and in a transparent manner in relationship with Data Subject;

(2) *Purpose limitation* - Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(3) *Data minimisation* - Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(4) *Accuracy* - Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure the personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ;

(5) *Storage limitation* - Personal Data must be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed;

(6) *Integrity and confidentiality* - Personal Data must be 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 and

organisational measures. The access to Personal Data has to take place on the basis of a proper authorisation and of a clear business need to know;

(7) *Accountability* - CIDP shall be responsible for, and be able to demonstrate compliance with GDPR and MDPA.

2.2. Information Notice

In order to comply with the principle of *fair and transparent processing,* the CIDP has to inform Data Subjects about the processing of their personal data, unless already informed.

The Information communicated shall include all the information provided under GDPR and MDPA, as follows:

(a) the identity and the contact details of CIDP
(b) the contact details of the Data Protection Officer
(c) the purposes of the processing for which the Personal Data are intended as well as the legal basis for processing
(d) categories of the personal data concerned
(e) legitimate interests pursued by the CIDP or by a third party
(f) the recipients or the categories of recipients of the Personal Data
(g) information on potential transfer of Personal Data to a third country or international organisation
(h) the period for which the Personal Data will be stored or if that is not possible, the criteria used to determine that period;
(i) the existence of the right to request from CIDP access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
(j) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on the consent before its withdrawal
(k) the right to lodge a complaint with the Mauritian Data Commissioner's Office
(l) where the provision of Personal Data is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as where the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
(m) the existence of automated decision-making where applicable, including profiling

If considered necessary for the processing to be fair and transparent, considering specific circumstances and specific context, CIDP may provide the Data Subject with additional information.

The Information must be provided in concise, transparent, intelligible and easily accessible way, using clear and plain language.

2.3. Legal basis of the processing

The CIDP must process Personal Data on the basis of one of the six legal grounds listed below:

(a) the Data Subject has given ***consent*** for the processing of his/her personal data for one of more specific purposes;
Consent has to be:
- *freely given* - real choice and control for Data Subject
- *specific* - separate consents for different purposes
- *informed* - providing information to Data Subject prior to obtaining the his/her consent in order to enable him/her to make informed decisions, understand to what he/she is agreeing to and exercise the right to withdrawal
- *unambiguous* - it is a mandatory affirmative act of Data Subject denoting an agreement to the processing of his/her Personal Data
- *explicit* - required in certain situations where serious data protection risk emerge (e.g. processing Special Categories of Personal Data)
- *demonstrable* - CIDP must prove that it has obtained valid consent from Data Subject
- *withdrawable* - Data Subject must have the right to revoke it at any time; it has to be as easy to withdraw as to give consent.

(b) processing is necessary for the performance of a contract to which the Data Subject is party or in order to take all the necessary steps at the request of the Data Subject prior to entering into a contract

(c) processing is necessary for compliance with a legal obligation to which the CIDP is subject

(d) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in CIDP

(f) processing is necessary for the purposes of the legitimate interests pursued by the CIDP or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

2.4. Data Subject Rights

GDPR and the MDPA provide a set of rights that may be exercised by Data Subjects:

(1) Right to access (Article 15 of GDPR)

The Data Subject has the right to obtain from CIDP confirmation as to whether or not Personal Data concerning him/her are being processed, and where that is the case, access to the Personal Data.
In case the access right is exercised by the Data Subject, CIDP has to provide the Data Subject with the set of mandatory information as provided by Article 15 of GDPR and a copy of the Personal Data undergoing processing.
Third parties (such as spouses of subjects) are not allowed to gain access to personal data without proper authorisation participating on studies.

(2) Right to rectification (Article 16 of GDPR)

The Data Subject has the right to obtain from CIDP without undue delay the rectification of inaccurate personal data concerning him/her. Taking in account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

(3) Right to erasure - *right to be forgotten* (Article 17 of GDPR)

The Data Subject has the right to obtain from CIDP, without undue delay, the erasure of his/her Personal Data in the following cases:

- the Personal Data are no longer necessary for the purposes for which they were collected or processed
- the Data Subject withdraws consent on which the processing is based and there is no other legal ground for processing
- the Data Subject objects to the processing based on legitimate interest and CIDP cannot demonstrate that there are overriding legitimate grounds for the processing
- Personal Data have been unlawfully processed
- Personal Data have to be erased for complying with a legal requirement which applies to the CIDP

The Right to be forgotten is subject to the mandatory retention period, which means that the CIDP may erase the Personal Data at the expiration of the mandatory retention period.

Nevertheless, following the Data Subject request, exercising the right to be forgotten before the expiring of the retention period, CIDP shall examine on a case by case basis the grounds for Data Subject Request, and implement measures so as to be able to selectively delete those Personal Data that the CIDP has no further right or obligation to process.

The CIDP may reject the request of the Data Subject, if:

(1) the request is received after the expiration of the retention period and the personal data is already deleted
(2) CIDP has a legal obligation, contractual obligations or another relevant overriding legal ground, to keep/process the personal data
(3) the personal data has to be processed for pre-litigation/litigation/any other legal dispute
(4) CIDP is requested to fulfil a requirement from an regulatory authority
(5) the personal data has to be processed for investigations/audits performed internally/externally or by an authority, started before the request was received

(4) Right to restriction of processing (Article 18 of GDPR)

Data Subject may ask to limit the processing of his/her Personal Data where one of the following applies:

(a) the accuracy of the Personal Data is contested
(b) the processing of the Personal Data is unlawful
(c) CIDP no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims
(d) the Data Subject has objected the processing, pending the verification whether the legitimate grounds of CIDP override those of the Data Subject

Where processing has been restricted, the Personal Data shall, with the *exception of storage*, only be processed by CIDP for:

(a) the exercise or defence of legal claims
(b) protecting the rights of another person or entity
(c) purposes that serve an important public interest

(d) other purposes that the Data Subject consents to

In case the restriction of processing was applied based on the Data Subject request, CIDP has the obligation to inform the Data Subject before the restriction of processing is lifted.

CIDP shall communicate any rectification or erasure of Personal Data or restriction of processing to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The CIDP shall inform the Data Subject about those recipients if the Data Subject requires it.

(5) Right to data portability (Article 20 of GDPR)

The Data Subject has the right to receive his/her Personal Data in a structured, commonly used and machine-readable format and to transmit those data to another CRO without hindrance from CIDP.
The Personal Data subject to portability have to be adequately secured and protected by the implementation of necessary technical means as to ensure the correct and secure transfer, as well as confidentiality and integrity of the transferred data.

The right to data portability shall not adversely affect the rights and freedoms of other rights.

(6) Right to object (Article 21 of GDPR)

The Data Subject may object to the processing of his/her Personal Data in the following cases:
(a) direct marketing, including profiling that is related to direct marketing;
(b) processing based on legitimate interests, including profiling that is related to such;
(c) processing for purposes of scientific or historical research and statistics.

In case of objection to processing, the CIDP must cease the processing, unless it can demonstrate that:

- it processes the Personal Data on the grounds of legitimate interests which override the fundamental rights and freedoms of the Data Subject (e.g. reasons of public interest) - such processing must be thoroughly documented;
- the processing is necessary for the establishment, exercise or defence of a legal claim.

(7) Automated decision - making including profiling (Article 22 of GDPR)

The Data subject has the right not to be subject to a decision based solely on automated processing, including profiling, except when the processing is:

necessary for entering into, or performance of, a contract between the Data Subject and CIDP
authorized by EU or Member State Law to which CIDP is subject
is based on Data Subject explicit consent

In such case, CIDP shall:
implement suitable measures to safeguard the Data Subject rights and freedoms and legitimate interests

- suitable information of the Data Subject about his/her rights, at least the right to obtain human intervention on the part of CIDP, to express his/her point of view and to contest the decision

In order to allow the Data Subject to exercise his/her rights, CIDP has put in place internal procedures for handling the requests received from the Data Subjects.

2.5. Retention period

Personal Data shall not be retained for longer than necessary in relation to the purposes for which they are further processed.

In pursuance of the afore mentioned principle, CIDP establishes the maximum period of time to lawfully retain Personal Data. Such retention periods are established in accordance with the legal requirements applicable to the CIDP, as well as in accordance with the best practices existing on the relevant market.

Beyond the retention periods, the Personal Data shall be erased or pseudonymised in an irreversible way in such a manner that the Data Subject can no longer be identified. Archiving shall not be considered erasure of Personal Data.

The principle of storage limitation shall also apply to Personal Data which are kept on paper. Such shall be erased by destruction of the paper support using for instance shredder devises which do not allow the reconstruction of the document which contains Personal Data unless an alternative destruction method was agreed.

2.6. Accountability

2.6.1. Data Protection Officer responsibilities

The DPO is responsible for:

(a) advising the management and its staff of its obligations under GDPR
(b) monitoring compliance with this Regulation and other relevant data protection law, the policies with respect to this and monitoring training and audit activities related to GDPR compliance
(c) to provide advice where requested on data protection impact assessments
(d) to cooperate with and act as the contact point for the Data Commissioner's Office
(e) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The DPO is not personally responsible for non-compliance with GDPR requirements. Each employee has the responsibility to comply with the requirements of GDPR and the data protection internal rules of the employer.

2.6.2. Staff responsibilities

Staff members who process personal data about subjects, staff, any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) all personal data is kept securely
(b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
(c) personal data is kept in accordance with the CIDP retention schedule
(d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer
(e) any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the Security Incident team (GDPR team) in resolving breaches
(f) where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer.

Where members of staff are responsible for newly employed staff or trainees doing work which involves the processing of personal information they must ensure that they are aware of the Data Protection principles.

2.6.3. Third-Party Data Processors

Where external companies are used to process personal data on behalf of CIDP, responsibility for the security and appropriate use of that data remains with CIDP.
Where a third-party data processor is used:

(a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
(b) the Data Processor shall not engage another processor without the prior written approval of the CIDP;
(c) reasonable steps must be taken that such security measures are in place;
(d) a written contract establishing what personal data will be processed and for what purpose must be set out;
(e) a data processing agreement must be signed by both parties.

2.6.4. Data processing through Joint-Controllers

In case CIDP determines together with another contractual partner the purposes and the means of processing, parties become Joint-Controllers.

When processing the Personal Data together with Joint-Controllers, CIDP has to sign a specific agreement (e.g. Data Processing Agreement - DPA), by which the parties, in a transparent way shall determine their responsibilities for compliance with GDPR requirements (e.g. duties in providing the transparent information to Data Subjects, designation of a contact person, unless a legal provisions in place determines the specific responsibilities of each of the Joint-Controllers.

2.6.5. Transfers / Disclosure of Personal Data to third countries

In case the Data Processor / Joint - CIDP is situated in a third country or the personal data is transferred/disclosed to an international organization situated in a third country, CIDP shall ensure that the requirements of Chapter V of GDPR are fully observed and shall ensure that such transfer/disclosure of Personal Data may take place only after the CIDP verifies the following:

(a) the transfers are based on an adequacy decision (Article 45 of GDPR);
(b) the transfers are subject to appropriate safeguards (Article 46 of GDPR);
(c) there are binding corporate rules in place (Article 47 of the GDPR) ;
(d) there are derogations for specific situations in place (Article 49);
(e) there are cases of transfers / disclosures which are nor authorized by EU law (Article 48 of GDPR).

2.6.6. Security measures

CIDP implements appropriate technical and organizational measures in order to ensure the secure processing of personal data, as well as in order to protect the Personal Data against unauthorized or unlawful processing.

For detailed information, please refer to specific internal procedures.

CIDP shall take all the appropriate measures in order to ensure the security of Personal Data.

2.6.7. Record of processing activities

Having in view that CIDP is processing Personal Data that is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, and the processing includes special categories of data, it is mandatory for the CIDP to keep a Record of processing activities.

The CIDP maintains a Record of processing activities which represents an overview of the Special Personal Data processing activities and contains all the information referred to in Article 30 of the GDPR.

The Record of processing activities is kept in a centralized manner and is operated by a designated CIDP Representative.

The Register of processing activities represents a picture in time of the processing activities. It shall be completed/modified each time a new Personal Data activity / an amendment to an existing one / ceasing of a processing activity occur. Each modification shall be time stamped.

The Register of processing activities is kept on in a secure manner, being accessed only by the responsible CIDP representative.

For avoidance of any doubt, the Register of processing activities is operated by the CIDP representative, nevertheless, he/she will be able to operate it only after receiving the relevant information and necessary approvals from the processing operation owner for which the latter is held solely responsible.

2.6.8. Data Breach Notification

CIDP has in place internal norms as to ensure the due notification of the supervision authorities, as well as well as of the Data Subjects.

2.6.9. Data Protection Impact Assessment

CIDP has in place internal norms as to carry out an assessment of the impact of the envisaged processing activities/operations on the protection of the Personal Data.

3. Sanctions

The sanctions provided by GDPR in case of infringements of the legal provisions may consist of:
i. Warning
ii. Reprimand
iii. Fines