



CHARLES TELFAIR COMPANY LTD

PRIVACY POLICY & PROCEDURES

Contents

1	Policy Statement.....	4
2	Purpose.....	5
3	Scope	5
4	Objectives	5
5	Definitions	6
6	Data Protection Background	9
6.1	General Data Protection Regulation (EU 2016/679).....	9
6.2	Mauritius Data Protection Act 2017 (Act No 20. of 2017).....	9
6.3	Personal Data	9
6.4	The Data Protection Principles	9
6.5	The Data Protection Commissioner	10
6.6	Data Protection Committee/ Officer.....	11
7	Governance Procedures	12
7.1	Accountability & Compliance	12
	7.1.1 Privacy by Design	12
	7.1.2 Information Assessment.....	13
7.2	Legal Basis for Processing (Lawfulness).....	14
	7.2.1 Processing Special Categories of Personal Data.....	14
	7.2.2 Records of Processing Operations.....	15
7.3	Third-Party Processors.....	15
7.4	Data Retention & Disposal	16
8	Data Protection Impact Assessments.....	17
9	Data Subject Rights Procedures	18
9.1	Consent & The Right to be Informed	18
	9.1.1 Consent Controls	19
	9.1.2 Alternatives to Consent	20
	9.1.3 Information Provisions	20
9.2	Privacy Policy & Notices	21

9.3	Personal Data not obtained from the Data Subject	21
9.3.1	Employee Personal Data	22
9.4	The Right of Access	22
9.4.1	Subject Access Request	22
9.5	Data Portability	23
9.6	Rectification & Erasure	24
9.6.1	Correcting Inaccurate or Incomplete Data	24
9.6.2	The Right to Erasure	25
9.7	The Right to Restrict Processing	25
9.8	Objections and Automated Decision Making	26
10	Oversight Procedures	27
10.1	Security & Breach Management	27
10.2	Passwords	28
11	Transfers & Data Sharing	28
12	Monitoring	28
13	Training	29
14	Penalties	29
15	Responsibilities	29

CHARLES TELFAIR COMPANY LTD Privacy Policy in terms of the General Data Protection Regulation (GDPR) and the Mauritius Data Protection Act (DPA)	
Scope of policy	This policy applies to Charles Telfair Company Ltd.
Policy operational date	11/11/2025
Policy prepared by	BDO
Date approved by Data Protection Committee	11/11/2025
Next policy review date	11/11/2026

1 POLICY STATEMENT

Charles Telfair Company Ltd (hereafter “**CTE**”) forms part of Eclasia Group (hereafter “**the Group**”) which is a respected, diversified and robust group in the Mauritian economic landscape whose activities are regrouped into six sectors: Food, Commerce, Logistics, Business Services, Education, and Hotels & Leisure. The Group expanded and operates in Africa and in the Indian Ocean region, mostly in Madagascar.

The Charles Telfair Campus stands today as a fully-fledged university with over 20 years of experience in the management and delivery of international tertiary education programmes. In addition to operating Curtin Mauritius in a 15 years’ partnership, Charles Telfair Campus manages a number of international programmes from South and North Metropolitan TAFE in Western Australia. It also operates the Charles Telfair Institute which has its own diploma and degree awarding powers. Curtin Mauritius is now ideally positioned to deliver best-in-class teaching and world-class research in Mauritius and the broader region. Curtin Mauritius works closely with the private sector and different Mauritian organizations to prepare its students to step in their future careers from the moment they graduate. Internships, networking, and seminars are systematically organized to that end. Curtin Mauritius not only attracts Mauritians but students from Madagascar, Comoros, Zimbabwe, Zambia, Kenya, and South Africa among others.

We need to collect personal data to effectively carry out our everyday business functions and activities and to provide the services in connection with our business. Such data is collected from employees, recruiting agents, students, responsible parties of children attending our nursery school/ preschool as well as from suppliers, and includes (*but is not limited to*), name, address, email address, date of birth, identification numbers, private and confidential information, special categories of personal data, bank details and other financial information.

CTE has elected to conform with the **European Union General Data Protection Regulation 2016** (hereafter the “**GDPR**”) and the **Mauritius Data Protection Act 2017** (hereafter the “**DPA**”) for all processing of personal data despite the operational jurisdiction or residential jurisdiction of a data subject. CTE is committed to processing all personal information in accordance with the GDPR and the DPA and any other relevant data protection laws (herein collectively referred to as the “**data protection laws**”).

CTE has put in place policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, and internal assessments. Ensuring and maintaining the security and confidentiality of personal and/or special categories of personal data is one of our top

priorities and we are proud to operate a '*Privacy by Default and by Design*' approach, assessing changes and their impact from the start and designing systems and processes to protect personal data at the core of our business.

2 PURPOSE

The purpose of this policy is to ensure that CTE meets its legal, statutory and regulatory requirements under the data protection laws, to ensure that all personal and special categories of personal data is processed compliantly and in the data subjects' best interests, and to achieve consistency across all relevant parts of the Group.

The data protection laws include provisions that promote accountability and governance and as such CTE has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3 SCOPE

This policy applies to all staff within CTE (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with CTE), and pertains to the processing of personal data. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 OBJECTIVES

CTE ensures the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their data protection rights. CTE has developed the below objectives to meet data protection obligations and to ensure continued compliance with the regulatory requirements.

CTE ensures that: -

- We protect the rights of individuals with regards to the processing of personal data;
- We develop, implement and maintain a privacy policy, procedure and training program for compliance with the data protection laws;
- Every business practice, function and process carried out by CTE, is monitored for compliance with the data protection laws and its principles;
- Data is only processed where we have met the lawfulness of processing requirements;
- We only process special category of data in accordance with the GDPR and the DPA;
- We record consent at the time it is obtained and evidence such consent to a Supervisory Authority where requested;

- We have robust and documented complaint handling and data breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection;
- We have a Data Protection Committee which takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out in 6.7;
- We provide clear lines of reporting and supervision with regards to data protection;
- We store and destroy all personal data, in accordance with the data protection laws timeframes and requirements;
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- Employees are aware of their own rights under the data protection laws and are provided with an employee privacy policy;
- Where applicable, we maintain records of processing activities in accordance with the Article 30 of the GDPR requirements and Section 33 of the DPA;
- We have developed and documented appropriate technical and organisational measures and controls for personal data security.

5 DEFINITIONS

- **‘Eclosia Group’** means all companies included in the Eclosia Group, including all subsidiaries & affiliates;
- **‘personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural 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, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **‘special categories of personal data’**, in relation to a data subject, means personal data pertaining to his racial or ethnic origin, his political opinion or adherence, his religious or philosophical beliefs, his membership of a trade union, his physical or mental health or condition, his sexual orientation, practices or preferences, his genetic data or biometric data uniquely identifying him, the commission or alleged commission of an offence by him, any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the

proceedings, or such other personal data as the Data Protection Commissioner may determine to be sensitive personal data.

- **‘genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **‘biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;
- **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **‘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;
- **‘restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future;
- **‘profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- **‘controller’** 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; where the purposes and means of such processing are determined by law, the controller or the specific criteria for its nomination may be provided for by law;
- **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **‘recipient’** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in

accordance with law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- **‘third party’** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **‘consent’** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **‘representative’** means a natural or legal person established in the European Union (hereafter "EU") who, designated by the controller or processor in writing, represents the controller or processor with regard to their respective obligations under the GDPR;
- **‘enterprise’** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **‘supervisory authority’** means an independent public authority which is established by an EU Member State. In Mauritius, it is the Data Protection Office;
- **‘supervisory authority concerned’** means a supervisory authority which is concerned by the processing of personal data because:
 - (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
 - (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
 - (c) a complaint has been lodged with that supervisory authority;
- **‘cross-border processing’** means processing of personal data which takes place in the context of the activities of establishments in more than one country, where the controller and processor is not in the established in the same country;
- **‘international organisation’** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

- **'data protection committee'** means The Data Protection Committee of CTE which consists of a designated Data Protection Officer and representatives from different departments.

6 DATA PROTECTION BACKGROUND

6.1 General Data Protection Regulation (EU 2016/679)

The GDPR was approved by the European Commission in April 2016 and applies to all EU Member States as from 25th May 2018. As a *'Regulation'* rather than a *'Directive'*, its rules apply directly to the Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

6.2 Mauritius Data Protection Act 2017 (Act No 20. of 2017)

The DPA was voted by the Mauritius Parliament in December 2017. The DPA is an accomplished effort to sustain and strengthen the control and personal autonomy of data subjects over their personal data. It has been designed to align with the key principles found in international laws namely the GDPR.

6.3 Personal Data

Information protected under the GDPR & DPA is known as **'personal data'**.

CTE ensures that a high level of care and measures are afforded to personal data falling within the GDPR's and DPA's **'special categories of personal data'** (previously **sensitive personal data**), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the **'special categories of personal data'**, the GDPR advises that such processing shall be prohibited unless one of the Article 9 clauses applies, as detailed in Clause 7.2.1.

6.4 The Data Protection Principles

The data protection laws require that personal data shall be: -

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject (***'lawfulness, fairness and transparency'***);
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes (***'purpose limitation'***);

- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**);
- 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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);
- 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 (**'integrity and confidentiality'**).

Article 5(2) of the GDPR requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* (**'accountability'**) and requires that firms **show how** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

6.5 The Data Protection Commissioner

Sections 14 & 15 of the DPA requires the following:

14. Subject to section 44, no person shall act as controller or processor unless he or it is registered with the Commissioner.

15. Application for registration

(1) Every person who intends to act as a controller or processor shall apply to the Commissioner, in such form as the Commissioner may approve, to be registered as controller or processor.

(2) Every application under subsection (1) shall be accompanied by the following particulars regarding the applicant–

(a) name and address;

(b) if he or it has nominated a representative for the purposes of this Act, the name and address of the representative;

(c) a description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate;

(d) a statement as to whether or not he or it holds, or is likely to hold, special categories of personal data;

(e) a description of the purpose for which the personal data are to be processed;

(f) a description of any recipient to whom the controller intends or may wish to disclose the personal data;

(g) the name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer the data; and

(h) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data.

The Data Protection Office is a public office which acts with complete independence and impartiality and it is not subject to the control or direction of any other person or authority in the discharge of its functions. The head of the office is the Data Protection Commissioner.

CTI is registered with the Data Protection Office and appears on the Data Protection Office Register as a controller and a processor of personal data.

6.6 Data Protection Committee/ Officer

Section 22(2)(e) of the DPA requires that every Controller of personal data in Mauritius shall appoint a Data Protection Officer (hereafter “DPO”) who will be responsible for data protection compliance issues.

CTI has a Data Protection Committee (hereafter “DPC”) which consists of a designated DPO and representatives from different departments. The DPC shall be responsible for all GDPR and DPA related topics in the European and Mauritian jurisdictions. ***To avoid any confusion, we will refer to both these positions as a Data Protection Committee in all our communications.***

The responsible persons of the DPC can be contacted in writing on dpc@telfair.ac.mu.

The DPC will be responsible to:

- Inform and advise the Controller/Processor and its employees about their obligation to comply with the DPA and other data protection laws;
- Monitor compliance with the DPA, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits;
- Be the first point of contact for the Data Protection Office and for individuals whose data are processed;
- Liaise with data subjects and the Data Protection Office in relation to any alleged breaches of GDPR and the DPA;
- Ensure that this Policy is regularly reviewed and updated as necessary;

- Monitor systems and procedures to ensure compliance with data protection laws and its principles;
- Take decisions with regards to data protection issues;

Any questions on the GDPR and the DPA should be addressed to the DPC.

7 GOVERNANCE PROCEDURES

7.1 Accountability & Compliance

Due to the nature, scope, context and purposes of processing of data undertaken by CTE, we have implemented adequate and appropriate technical and organisational measures to ensure the collection and safeguarding of personal data is compliant with the data protection laws that we have obligations under.

We can demonstrate that all processing activities are performed in accordance with the data protection laws and that we have in place robust policies, procedures, measures and controls for the protection of data.

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance;
- Provide a dedicated and effective data protection training program for all staff;
- Identify key senior stakeholders to support the data protection compliance program;
- Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role;
- Identify, create and disseminate the reporting lines within the data protection governance structure.

The technical and organisational measures that CTI has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies.

7.1.1 Privacy by Design

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have additional measures in place to adhere to this ethos, including: -

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be 'limited to what is necessary', which forms the basis of our minimal approach. We only ever obtain, retain,

process and share the data that is essential to carry out our services and legal obligations and we only keep it for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collections (i.e. forms, website, surveys etc) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain;
- Physical collection (i.e. agreements or client contracts) is checked against the minimum requirements and only that which is relevant and necessary is collected;
- We have documented destruction procedures in place as detailed in Clause 7.4, where a data subject or third-party provides us with personal data that is a surplus to the requirements of the GDPR;
- We have service level agreements and bespoke agreements in place with third-party controllers who send us personal data (either in our capacity as a Controller or Processor). These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.

Restriction

Our *Privacy by Design* approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of CTE's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal data. Special categories of personal data are restricted at all levels and can only be accessed by authorised staff of CTE.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (e.g. employee's special categories of personal data). Such paper format documents are stored in secure locked cupboards and are confidentially shredded once the requirement for retention has come to an end.

7.1.2 Information Assessment

To enable CTE to fully prepare for and comply with the data protection laws, we have carried out a company-wide data protection information assessment to better enable us to record, categorise and protect the personal data that we hold and process.

The assessments have identified, categorised and recorded all personal data obtained, processed and shared by CTE in its capacity as a Controller/Processor. They have been compiled on a Record of Processing Operations sheet as detailed in Clause 7.2.2., as well as a Digital Devices Inventory which include the format on which the personal data is stored.

7.2 Legal Basis for Processing (Lawfulness)

At the core of all personal data processing activities undertaken by CTE, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the data protection laws.

This legal basis is documented on our Record of Processing Operations sheet and where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. Personal data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The data subject has given consent to the processing of their personal data for one or more specific purposes; or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which we are subject; or
- Processing is necessary for the purposes of the legitimate interests pursued by CTE or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).

7.2.1 Processing Special Categories of Personal Data

We will only ever process special categories of personal data where:

- The data subject has given explicit consent to the processing of the personal data;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- Processing relates to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Where CTE processes personal data that falls into one of the above categories, we have the specified provisions and measures in place prior to any processing.

Measures include:

- Ensuring that one of the above permissions is in place before processing the special categories of personal data;
- Having an appropriate policy document in place when the processing is carried out, specifying our:
 - procedures for securing compliance with the data protection laws principles;
 - policies as regards the retention and erasure of personal data processed in reliance on the condition;
 - retention periods and reason (*i.e. legal, statutory etc*);
 - procedures for reviewing and updating our policies in this area.

Please refer to our Records Management Policy for further guidance and procedures.

7.2.2 Records of Processing Operations

Section 33 of the DPA provides that “every controller or processor shall maintain a record of all processing operations under his or its responsibility”. It is therefore mandatory to keep a Record of Processing Operations sheet which includes:

- What personal data we hold;
- Where it came from;
- Who we share it with;
- Legal basis for processing it, etc.

7.3 Third-Party Processors

CTE may utilise external processors for certain processing activities. Such external processing includes (but is not limited to): -

- IT Systems and Services, including, email hosting and support services;
- Payroll services
- Collecting and shredding of papers containing personal data;
- Printing and advertising of brochures for CTE.

We have strict due diligence procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain all necessary information to ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

Where possible, we do enter in a Controller and Processor Agreement to ensure that the third-party processors comply with data protection laws.

Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

Our third-party contracts stipulate, in particular, that the processor: -

- Processes the personal data only on our documented instructions;
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject);
- Shall inform us of any such legal requirement to transfer data before processing;
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Takes all measures to secure the personal data at all times;
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights;
- Assists CTE in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments;
- When requested, deletes or returns all personal data to CTI after the end of the provision of services relating to processing, and deletes existing copies where possible;
- Makes available to CTE, all information necessary to demonstrate compliance with the obligations set out here and, in the contract;
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract;
- Informs CTE immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract.

7.4 Data Retention & Disposal

CTE has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and business requirements, as well as adhering to the data protection laws requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data at all times.

Please refer to our Records Management Policy for full details on our retention, storage periods and destruction processes (amongst others).

8 DATA PROTECTION IMPACT ASSESSMENTS

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by CTE. We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where CTE is in the future considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedom of data subjects, we always carry out a Data Protection Impact Assessment (hereafter “**DPIA**”) (sometimes referred to as a Privacy Impact Assessment).

Pursuant to Article 35(3) and Recitals 84, 89-96 of the GDPR, and guidance issued by the Data Protection Office, we consider processing that is likely to result in a high risk to include: -

- Evaluation or scoring personal aspects/behaviour of people including profiling;
- Automated decision-making producing legal or similar significant effects;
- Systematic monitoring by observing, monitoring or controlling data subjects (i.e. CCTV);
- Processing on a large scale of special categories of personal data;
- Processing on a large scale of personal data relating to criminal convictions and offences;
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects;
- Processing involving the innovative use or application of new technological or organisational solutions;
- When the processing “prevents data subjects from exercising a right or using a service or a contract”;
- Matching or combining data sets, for instance, where personal data collected for one or more purposes are compared with personal data collected for any other purpose;
- Processing personal data on vulnerable persons to whom the data relates (e.g. people with mental illness, asylum seekers or elderly people, patients, children, etc.).

Carrying out DPIAs enables us to identify the most effective way to comply with the data protection laws and ensure the highest level of data privacy when processing. It is part of

our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

9 DATA SUBJECT RIGHTS PROCEDURES

9.1 Consent & The Right to be Informed

The collection of personal and special categories of personal data is a fundamental part of the business of CTE and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

Where processing is based on consent, CTE has reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms;
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes;
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data;
- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand;
- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and is not be a precondition of any service (unless necessary for that service);
- Along with our company name, we also provide details of any other third party who will use or rely on the consent;
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case;
- Pre-ticked, opt-in boxes are never used;
- We keep detailed records of consent and can evidence at a minimum: –
 - that the individual has consented to the use and processing of their personal data;
 - that the individual has been advised of our company name and any third party using the data;
 - what the individual was told at the time of consent;
 - how and when consent was obtained;

- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
 - Opt-out links in mailings or electronic communications;
 - Opt-out process explanation and steps on website and in all written communications;
 - Ability to opt-out verbally, in writing or by email;
- Consent withdrawal requests are processed immediately and without detriment;
- Processing personal data of children, age-verification and parental-consent measures have been developed and are in place to obtain consent;
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents;
- For special categories of personal data, the consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified.

9.1.1 Consent Controls

CTE maintains records of data subject to consent for processing personal data and is always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the DPC prior to being circulated. The same written declaration consent will include details of how to withdraw consent.

Consent to obtain, process, store and share (*where applicable*), is obtained by CTE through:

-

- In Writing;
- Email;

CTE uses checklists and signed customer agreements, to ensure that consent has been obtained and to remind employees of their additional consent obligations.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

9.1.2 Alternatives to Consent

CTE recognises that there are other lawful bases for processing of data and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

9.1.3 Information Provisions

Where personal data is obtained directly from the individual (i.e. through consent, by employees or students, written materials and/or electronic formats (i.e. website forms, email etc)), we provide the below information in all instances, in the form of a consent/privacy notice: -

- The identity and the contact details of the Controller and, where applicable, of the Controller's representative;
- The contact details of our DPC;
- The purpose(s) of the processing for which the personal information is intended;
- The legal basis for the processing;
- Where the processing is based on point (f) of Article 6(1) of the GDPR "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party", details of the legitimate interests;
- The recipients or categories of recipients of the personal data (if applicable);
- If CTE intends to transfer the personal data to a third country or international organisation without an adequate decision by the Data Protection Office, reference to the appropriate or suitable safeguards CTE has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request 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;
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2) of the GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a Supervisory Authority;
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the GDPR and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored in accordance with our Records Management Policy unless there is a legal requirement to keep the information longer.

9.2 Privacy Policy & Notices

This document is our **Privacy Policy** and is an internal document designed to define CTE's controls, procedures and objectives for securing, processing, handling and protecting personal information and complying with the data protection laws.

CTE uses the term Privacy Notice which is a separate document from our Privacy Policy and is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly).

9.3 Personal Data not obtained from the Data Subject

Where CTE obtains and/or processes personal data that has **not** been obtained directly from the data subject, CTE ensures that the information is provided to the data subject within 30 days of our obtaining the personal data (*except for advising if the provision of personal data is a statutory or contractual requirement subject to the conditions set out below*).

In addition to the information provided in the Data Subjects Rights section of this Policy, we also provide information about: -

- The categories of personal data;
- The source the personal data originated from and whether it came from publicly accessible sources.

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure. Where CTE intends to further process any personal data for a purpose **other** than that for which it was originally obtained, we communicate this intention to the data subject prior to doing so and where applicable, process only with their consent.

Whilst we follow best practices in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information;

- The provision of such information proves impossible and/or would involve a disproportionate effort;
- Obtaining or disclosure is expressly laid down by law to which CTEI is subject and which provides appropriate measures to protect the data subject's legitimate interest;
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by laws, including a statutory obligation of secrecy.

9.3.1 Employee Personal Data

Our Employee Privacy Policy ensures that employees are provided with the appropriate information disclosure and are aware of how we process their data and why. The Employee Privacy Policy also informs employees of their rights under the data protection laws and how to exercise these rights.

Please refer to our Employee Privacy Policy for more details.

9.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 of the GDPR and any communication under Articles 15 to 22 and 34 of the GDPR and Sections 37 to 40 of the DPA (collectively, referred to the “**Rights of Data Subjects**”), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject’s identity (*i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with a Supervisory Authority.

9.4.1 Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing;
- The categories of personal data concerned;

- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- If the data has or will be disclosed to third countries or international organisations and the appropriate safeguards pursuant to the transfer;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a Supervisory Authority;
- Where personal data has not been collected by CTE from the data subject, any available information as to the source and provider;
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Subject Access Requests (hereafter “**SAR**”) are passed to the DPC as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Assessment to see the format in which it is held in, with whom it has been shared and any specific timeframes for access.

SARs are always completed within 30 days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our Data Subject Access Request Policies and Procedures for the guidelines on how a SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

9.5 Data Portability

CTE provides all personal data pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the GDPR concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1) of the GDPR;

- Consent pursuant to point (a) of Article 9(2);
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means.

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from CTE to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- HTML;
- CSV;
- XLSX;
- DOCX;
- PDF.

All requests for information to be provided to the data subject or a designated controller are done free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to a Supervisory Authority.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

9.6 Rectification & Erasure

9.6.1 Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d) of the GDPR, all data held and processed by CTE is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller informs us that the personal data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The DPC is notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data

in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to a Supervisory Authority.

9.6.2 The Right to Erasure

This right is also known as *'The Right to be Forgotten'*. CTE complies fully with Article 5(e) of the GDPR and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by CTE is categorised when assessed by the Information Audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Records Management Policy for exact procedures on erasing data and complying with the Article 17 of the GDPR requirements.

9.7 The Right to Restrict Processing

There are certain circumstances where CTE restricts the processing of personal data, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the Information Audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

CTE will apply restrictions to data processing in the following circumstances: -

- Where an individual contests the accuracy of the personal data and we are in the process of verifying the accuracy of the personal data and/or making corrections;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual;
- When processing is deemed to have been unlawful, but the data subject requests restriction as opposed to erasure;
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim.

The DPC reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted,

and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to a Supervisory Authority.

9.8 Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online.

Individuals have the right to object to: -

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling);
- Processing for purposes of scientific/historical research and statistics.

Where CTE processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on '*grounds relating to their particular situation*'. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- The processing is for the establishment, exercise or defence of legal claims.

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, CTE will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. CTE understands that decisions absent of

human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the GDPR, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing;
- It produces a legal effect or a similarly significant effect on the individual.

In limited circumstances, CTE will use automated decision-making processes within the guidelines of the GDPR. Such instances include: -

- Where it is necessary for entering into or performance of a contract between us and the individual;
- Where it is authorised by law (e.g. fraud or tax evasion prevention);
- When based on explicit consent to do so;
- Where the decision does not have a legal or similarly significant effect on someone.

Where CTE uses automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

10 OVERSIGHT PROCEDURES

10.1 Security & Breach Management

Alongside our *'Privacy by Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our ***IT Policies & Procedures manual*** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, CTE has dedicated controls and procedures in place for such situations, along with the notifications to be made to a Supervisory Authority and data subjects (where applicable).

Please refer to our Data Breach Response Plan & Procedures for specific protocols.

10.2 Passwords

Passwords are a key part of CTE protection strategy and are used throughout CTE to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach. Whilst passwords are also directly related to Information Security and Access Control, CTE recognises that strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third parties who are responsible for one or more account, system or have access to any resource that requires a password. Full procedures and guidelines for passwords, access and security can be found in our ***IT Policies and Procedures Manual***.

11 TRANSFERS & DATA SHARING

CTE takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Whenever personal data is transferred across borders, CTE conforms with the requirements of the data protection laws regardless of the jurisdictions.

Please refer to our Data Sharing Procedures where personal data is shared with third parties who are not processors, for further details.

12 MONITORING

This policy details the extensive controls, measures and methods used by CTE to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct.

In addition to these, we also carry out compliance monitoring processes, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The DPC has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Executive Director where applicable.

Data minimisation methods are frequently reviewed, and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

13 TRAINING

Through our strong commitment and robust controls, we ensure that all staff have access to and can easily interpret the data protection laws requirements and its underlying principles and that they have ongoing training and support to demonstrate knowledge, competence and adequacy for their role.

14 PENALTIES

CTE understands its obligations and responsibilities under the data protection laws and Supervisory Authority and comprehend the severity of any breaches under the data protection laws. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the data protection laws, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. **We recognise that:** -

- Under GDPR, breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher;
- Under GDPR, breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing requirements or non-compliance with an order by a Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher;
- Under DPA, in case of breaches of the applicable data protection laws, a fine not exceeding MUR 200,000 and imprisonment for a term not exceeding 5 years may be imposed.

15 RESPONSIBILITIES

CTE has a DPC which consists of a designated DPO. The DPC's role is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPC has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special categories of personal data will be provided with data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledgeable for the role they undertake.