Data Protection Policy - TLC 08 July 2020

Contents

Introduction 2

Definitions – to check all used in the policy 3

Policy 6

- Governance 6
- Principles 6
- Data Collection 7
- Data Processing 7
- Special Categories of Data 8
- Data Quality 9
- Direct Marketing 9
- Retention 10
- Data Protection 10
- Data Subject Requests 10
- Law Enforcement Requests & Disclosures 12
- Data Protection Training 12
- Data Transfers 12
  - Transfers to Third Parties 13
- Complaints Handling 13
- Breach Reporting 13

Policy Maintenance 14

- Publication 14
- Effective Date 14
- Revisions 14

Related Documents 15

Appendix A- Adequacy for Personal Data Transfers 16

Introduction

The Tree of Life Centre ("TLC") is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of TLC Workers and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a TLC Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

TLC, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose TLC to complaints, regulatory action, fines and/or reputational damage.

TLC's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all TLC Workers and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

Definitions – to check all used in the policy

Employee	An individual who works part-time or full-time for TLC under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Third Party	An external organisation with which TLC conducts business and is also authorised to, under the direct authority of TLC, Process the Personal Data of TLC Contacts.
Personal Data	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Contact	Any past, current or prospective TLC customer.
Identifiable	Natural Person Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A 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 Subject	The identified or Identifiable Natural Person to which the data refers.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.

Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Consent	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.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.
Profiling	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Binding Corporate Rules	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Personal Data Breach	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.

Encryption	The process of converting information or data into code, to prevent unauthorised access.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Policy

Governance

United Churches Healing Ministry shall appoint a Data Protection Officer who will have responsibility for the oversight and outworking of the Data Protection Policy throughout the organisation. They will work with the relevant departmental managers to achieve this and ensure ongoing compliance with the necessary parts of the legislation.

The manager of each department will be responsible for ensuring that any personal data their department uses is processed according to the organisation's procedures and policy as well as the Data Protection principles, as stated below. Each department will undertake annual Data Audits to ensure that all data is tracked and the policy for retention and deletion is being stringently followed.

Principles

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, TLC must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means TLC must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means TLC must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and kept up to date. This means TLC must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be 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. This means TLC must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

Personal Data shall 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. TLC must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means TLC must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection

Personal Data should normally only be collected from the Data Subject.

If the Personal Data is collected from a Third Party then the Data Subject must be informed unless:

- The Data Subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation

TLC will provide Data Subjects with information as to the purpose of the Processing of their Personal Data before, or as soon as possible after, processing of that data commences. Where consent is needed, this will be obtained and documented beforehand.

Data Processing

TLC will only process data providing at least one of the following criteria are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject).

Should the Personal Data be needed to be further processed for purposes beyond the original purpose, an assessment will be made to determine the lawful basis for that further Processing, before and such Processing is commenced.

In any circumstance where Consent has not been gained for the specific Processing in question, TLC will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

Special Categories of Data

TLC will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained by the Data Protection Officer and the basis for the Processing clearly recorded with the Personal Data in question.

Where Special Categories of Data are being Processed, TLC will adopt additional protection measures.

Data Quality

TLC will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by TLC to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the Data Subject.
    - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

Direct Marketing

As a general rule TLC will not send promotional or direct marketing material to a TLC Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Anyone wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the Data Protection Officer.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

Retention

To ensure fair Processing, Personal Data will not be retained by TLC for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which TLC departments need to retain Personal Data is set out in their 'Personal Data Retention Schedule'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Each TLC department will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by each TLC department is provided in the TLC 'Information Security Policy'. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

Data Subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Restriction of Processing.
- Data portability.

- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, TLC will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.

The right of the Data subject to:

- object to Processing of their Personal Data.
- lodge a complaint with the Data Protection Authority.
- request rectification or erasure of their Personal Data.
- request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Data Protection Officer, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require TLC to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If TLC cannot respond fully to the request within 30 days, the Data Protection Officer shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).

- The name and contact information of the TLC individual who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Detailed guidance for dealing with requests from Data Subjects can be found in the TLC 'Data Subject Request Handling Procedures' document.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If a TLC department Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any TLC department receives a request from a court or any regulatory or law enforcement authority for information relating to a TLC Contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

Data Protection Training

All TLC Workers that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each TLC department will provide regular Data Protection training and guidance for their staff.

Data Transfers

TLC may transfer Personal Data to internal or Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection (see Appendix i) for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism (see Appendix i).

TLC may only transfer Personal Data where one of the transfer scenarios listed below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures

taken in response to the Data Subject's request.

- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

Transfers to Third Parties

Each TLC department will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, each TLC department will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, the TLC department will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, the TLC department will enter into, in cooperation with the Data Protection Officer, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with TLC instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

The Data Protection Officer shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the TLC Management team.

Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office.

Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Officer providing a

description of what occurred. Notification of the incident can be made via e-mail DPO@TLC.org, by calling 01484 461098, or by using the anonymous incident reporting form located in both offices.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the TLC Management Team will initiate an emergency response team to coordinate and manage the Personal Data Breach response.

Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the Data Protection via e-mail DPO@TLC.org.

Publication

This policy shall be available to all TLC Workers in the policies and procedures manual found in the main office or via alternative means as deemed appropriate by the Data Protection Officer.

Effective Date

This policy is effective as of May 2018

Revisions

The Data Protection Officer is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to TLC Workers through the personnel department. Changes to this policy will come into force when published and a revised copy is filed in the policies and procedures file.

Related Documents

Listed below are documents that relate to and are referenced by this policy.

- Procedure for Processing Data
- Subject Access Request Handling Procedure
- Data Protection Policy
- Data Retention Schedule
- Information Security Policy

Appendix A- Adequacy for Personal Data Transfers

The following are a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

- EU Countries (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)
- Iceland
- Liechtenstein
- Norway
- Andorra
- Argentina
- Canada (commercial organisations)
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- United States (Privacy Shield certified organisations)

The following are a list of Third Country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection. Appropriate safeguards

- Model Clauses
- Binding Corporate Rules
- Codes of Conduct
- Certification Mechanisms

Derogations

- Explicit Consent
- Compelling Legitimate Interests
- Important reasons of Public Interest
- Transfers in response to a foreign legal requirement
- DPA approved contracts between Data Controllers and Data Processors

----------END OF DOCUMENT----------

Document Revisions

Data Protection Policy - TLC			
Version	Description of Change	Date	Review Date
1.0	Document New	May 2018	
1.1	New format	July 2020	2021-07