GENERAL DATA PROTECTION REGULATIONS ("GDPR") POLICY

1. Definitions

'*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.

'*Sensitive personal data'* relates to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

'*Controller*' means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

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

'*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.

'*Supervisory authority'* refers to the data protection authority that has been identified as the lead supervisory authority, in this case the Data Protection Commissioner.

'*Compliance Manager'* refers to the individual who has been appointed to take responsibility for data protection compliance.

'*Third country'* refers to a country outside the European Economic Area (EEA).

2. Introduction

It is the policy of Dublin Maccabi Trust (the "Trust") to comply with the requirements of the Data Protection Acts 1988 to 2018 (the 'Acts') and the General Data Protection Regulations (the GDPR).

In the ordinary course of its business, the Trust may collect and store:

(i) personal data relating to employees and contractors;

(ii) personal data relating to Trustees of Dublin Maccabi Trust for the purposes of complying with the Company Act 2014. Trustees must ensure that any personal information collected, stored or processed by them for the above purposes is done in accordance with the Acts; and

3. Principles

Both the DP Acts and the GDPR seek to protect the rights of individuals with regard to the processing and use of their personal data. However, it is necessary to balance the rights of individuals with the rights of businesses to process personal data in the pursuit of their legitimate interests. In order to achieve this balance, the processing of personal data must be transparent, proportionate, fair and lawful.

The DP Acts and the GDPR set out the data protection principles that apply to the processing of personal data.

3.1. Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

3.2. Purpose limitation

Personal data shall be collected for specific, explicit and legitimate purpose(s) and not further processed in a manner incompatible with those purposes.

3.3. Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.4. Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

3.5. 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 are processed.

3.6. Integrity and 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, using appropriate technical or organisational measures.

4. Processing of Personal Data

The general rule under data protection law is that personal data must not be processed by a data controller unless the data controller complies with its obligations under the data protection principles and satisfies at least one of the prescribed preconditions for lawful processing of personal data.

The Trust is committed to only processing personal data if one, or more, of the following reasons applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) 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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or another natural person;
(e) 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 controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Processing of Special Categories of Personal Data

Under data protection law, the processing of special categories of personal data is prohibited. However, the Trust shall be permitted to process special categories of personal data if one of the following applies:

(a) the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes;
(b) 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;
(c) processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside the body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of

the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6. Data Subjects' Rights

The Trust shall take all appropriate measures ensuring that the guaranteed rights of data subjects are not infringed upon during the course of its processing activities. Under data protection law, data subjects are entitled to the exercise their rights. The Trust shall facilitate the wish, of a data subject, to exercise any one of these rights. The rights that data subjects are entitled to are set out in further detail below.

The Trust shall provide information on action taken on any request by a data subject to exercise their rights without undue delay and within one month of receipt of the request (this period may be extended by two months provided the data subject is notified). It will also assist a controller in fulfilling a subject access request.

6.1. Right of access by the data subject

Data subjects shall have the right to obtain from the Trust confirmation as to whether or not the personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

6.2. Right to rectification

Data subjects shall have the right to obtain from the Trust the rectification of inaccurate personal data concerning him or her.

6.3. Right to erasure ('right to be forgotten')

Data subjects shall have the right to obtain from the Trust the erasure of personal data concerning him/her where one of the following applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR;
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

The 'right to be forgotten' does not apply when the processing is necessary for:

(a) exercising the right of freedom of expression and information;
(b) compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of the GDPR;
(d) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) the establishment, exercise or defence of legal claims.

6.4. Right to restriction of processing

Data subjects shall have the right to obtain from the Trust restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the Trust no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

The Trust shall communicate any rectification or erasure of personal data or restriction of processing in accordance with clauses 6.2., 6.3. and 6.4. to each recipient to whom the personal data have been disclosed.

6.5. Right to data portability

Data subjects shall have the right to receive the personal data concerning him/her in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hinderance from the Trust where:

(a) the processing is based on consent or on a contract to which the data subject is party;

(b) the processing is carried out by automated means.

6.6. Right to object

Data subjects shall have the right to object to the processing of their personal data which is based on the legitimate interests pursued by the Trust or the performance of a task carried out in the public interest, including profiling based on these provisions. The Trust will no longer process the personal data unless it can be demonstrated that the legitimate grounds for processing the personal data override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Data subjects shall have the right to object to the processing of personal data where personal data are processed for direct marketing purposes.

6.7. Automated individual decision making, including profiling

Data subjects shall have the right to not be subject to a decision solely based on automated processing, including profiling, which produces legal effects or similarly significantly affects him/her. However, this will not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.

7. Data Transfers

Generally personal data cannot be transferred to third countries unless the country itself ensures an adequate level of data protection. The EU Commission has prepared a list of countries that are deemed to provide an adequate standard of protection and these include all countries within the European Economic Area (i.e. European Union member states, Norway, Iceland and Liechtenstein) as well as Switzerland, Argentina, Guernsey, and Isle of Man and to a limited extent Canada. With regard to the United States, those companies that have signed up to the 'Privacy Shield' arrangements will be regarded as having adequate levels of data protection and therefore transfers may take place to such companies.

If the country to which the data are to be sent does not provide such a standard of protection then the Trust, where it wishes to transfer information to such a country, may rely on alternative measures to ensure the safety of the data. If the data controller can point to one or more of the alternative measures, then the transfer of personal data to the third country may proceed. These alternative measures include, for example, that the transfer of personal data is required or authorised by law, or that the consent of the individual has been obtained to the transfer.

In the absence of consent for the transfer, a transfer is authorised where the controller can point to adequate data protection safeguards such as standard contractual clauses or binding corporate rules.

For the personal data that is transferred, it is transferred on the basis of an adequacy decision and can continue until such a decision is amended, suspended or repealed.

8. Agreements with Third Party Processors

Where processing is to be carried out on behalf of the Trust, it shall be governed by a contract (or some other legal act) that is binding on the processor. Such a contract shall set out (i) the subject-matter and duration of the processing; (ii) the nature and purpose of the processing; (iii) the type of personal data and categories of data subjects; and (iv) the obligations and rights of the controller. Such a contract or legal act shall stipulate that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32;
(d) respects the conditions for engaging another processor (Article 28 (2) & (4));
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Where a processor engages another processor (sub-processor) to carry out specific activities on behalf of the Trust, the same data protection obligations as set out in the contract between the Trust and the processor shall be imposed on that sub-processor by way of a contract (or some other legal act).

All of these measures are required under data protection law to ensure the ongoing security and confidentiality of processing activities that may affect individual data subjects. When in the process of engaging with a new processor, and in order to ensure that the rights of data subjects are protected, the Trust shall consult this document to ensure fulfilment of all the necessary requirements under data protection law.

9. Training

The Secretary will ensure that this document is kept up-to-date on behalf of the Trust. Training will be provided to Trustees where deemed necessary. The Secretary shall maintain records of training conducted.,

10. Audit

GDPR audits may be undertaken as required. Given the current nature, scale and purpose of the processing, an audit is not deemed necessary this year.

11. Data Breaches and Fines

The Trust maintains and shall continue to maintain an 'Internal Breach Register'. Any breaches, or suspected breaches, shall be recorded for internal use here.

In the event of a personal data breach, the Trust shall notify the personal data breach to the Data Protection Commissioner no later than 72 hours of having become aware of it. In its notification to the Data Protection Commissioner, the Trust shall use the 'Data Breach Notification Form' specifically created for this purpose. This form contains the following:

(a) description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) the name and contact details of the data protection manager or other contact point where more information can be obtained;
(c) description of the likely consequences of the personal data breach;
(d) description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Trust shall notify the personal data breach directly to the data subject without undue delay. Such a notification should contain at least points (b), (c) and (d) above. However, there are certain instances in which a notification to the data subject of a personal data breach is not required. These conditions are as follows:

(a) the Trust has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the Trust has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Fines imposed for contravention of the relevant data protection legislation can be severe. Currently, the maximum fine for non-compliance with the Data Protection Act is €100,000. However, under the GDPR this environment will be subject to significant change. Under the GDPR, there are two thresholds for administrative fines:

(i) 2% of an undertaking's global turnover in the previous year or €10 million, whichever is higher;
(ii) 4% of an undertaking's global turnover in the previous year or €20 million, whichever is higher.

12. Complaints

If there is a suspected breach of the data protection laws in relation to an individual, it may be investigated by the Data Protection Commissioner. The Data Protection Commissioner may investigate the suspected contravention whether the individual complains directly to him/her or if the Data Protection Commissioner is otherwise of the opinion that there may be a contravention. The Data Protection Commissioner may carry out such investigations as he/she considers appropriate. If the Data Protection Commissioner believes that there has been a contravention of the data protection laws, he/she may issue a notice in writing to the Trust. This notice may be served to a person/entity requiring them to take the necessary steps to rectify the situation and comply with all relevant components of data protection law. Failure to comply with the Data Protection Commissioner's advice and direction shall mean that the Trust shall be guilty of an offence, potentially leading to an administrative fine.

If a complaint, or a request, is received by the Company directly from an individual (data subject), the Trust shall follow all steps outlined in further detail in the Trust's 'Subject Access Request' procedure.

13. Retention of Records

In addition to maintaining proper records, the Trust is required to retain those records in line with various applicable laws and regulations including the Data Protection Acts, the GDPR and the Statute of Limitations. The Data Protection Acts and the GDPR stipulate that information should not be retained any longer than is necessary for the purposes for which it was obtained (data minimisation).

Section 886 of the Taxes Consolidation Act, 1997, as amended, provides that documents and records concerning income tax, corporation tax or capital gains tax should be retained for a period of 6 years from the date that the taxable event occurred.

Under the Statute of Limitations, 1957, a number of actions can be brought for a period of up to 6 years from the date of the cause of action. As a general rule, records relating to employees will be retained for a period of at least six years. The Trust shall implement appropriate technical and organisational measures to ensure the destruction of all records that have out-lived their relevant life cycles. Records relating to the advisors will be retained for a period of six years following termination of the relationship.

The Trust should be aware that there may be other areas of law and regulation (e.g. requirements of employment law) that are relevant for the purposes of a document retention policy. Professional advice should be sought in this regard.