PHILANTHROPY IRELAND

SHARE TODAY. SHAPE TOMORROW.

DATA PROTECTION POLICY

Date: 14 May 2018
Version: 2.0

TABLE OF CONTENTS

DATA PROTECTION POLICY

1. Introduction

1.1 Philanthropy Ireland ("**PI**"), based in 56 Fitzwilliam Square North, Dublin 2, is an independent association of philanthropic organisations and interests committed to the development of philanthropy and giving in Ireland. PI provides a collective voice for philanthropy, actively supporting strategic giving for positive impact.

1.2 In performing its functions, PI is required to collect, store and Process Personal Data within the meaning of (i) the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016), and (ii) the Data Protection Act 2018 (together, "**DP Law**").

1.3 PI respects the privacy rights of those about whom we Process Personal Data and we are conscious of our obligations under DP Law. In order to ensure a compliant and consistent approach to PI's obligations under DP Law, PI have instituted this Data Protection Policy (the "**Policy**").

2. Objectives

2.1 The objectives of the Policy are to:

(a) set the guidelines to ensure PI complies with the provisions of DP Law;

(b) establish ongoing compliance measures;

(c) identify key compliance requirements; and

(d) ensure that any shortfalls in compliance are identified and communicated to PI as required.

2.2 This Policy is also intended to provide evidence of PI's accountability for compliance with DP Law, as required by Article 5(2) GDPR.

2.3 This Policy is also intended to ensure that PI staff are aware of their responsibilities under DP Law. "**Staff**" means all PI personnel, including employees, consultants, contractors, interns and agents, both full and part-time, in whatever capacity they may work for or be engaged by PI.

2.4 Staff are obliged to comply with the terms of this Policy when Processing Personal Data on PI's behalf. Any breach of this Policy may result in disciplinary action.

3. **Key Principles**

3.1 In order to understand PI's obligations under DP Law, it is necessary to first set out some explanations of key principles under, and terms used in, DP Law.

(a) *Personal Data*

DP Law applies only to Personal Data, as defined in DP Law. This means any information relating to an identified or identifiable natural person. 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.

(b) *Special Categories of Personal Data*

"**Special Categories of Personal Data**" or "**Sensitive Data**", is Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and also includes 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. There are enhanced compliance requirements under DP Law on Controllers (as defined below), such as PI, who may Process Special Categories of Personal Data.

(c) *Processing*

"**Processing**" is defined very widely under DP Law and includes any activity involving the use 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.

DP Law places obligations on those who determine the purposes and means of Processing of Personal Data ("**Data Controller**" or "**Controllers**") while giving rights to those who are the subject of that data (the "**Data Subjects**"). A person who Processes data may either be a Controller or, where Personal Data is Processed on behalf of a Controller by another person (other than an employee), a data processor (a "**Data Processor**" or "**Processor**").

(d) *The Data Protection Commission*

The Data Protection Commission (the "**DPC**") is responsible for monitoring compliance with DP Law in Ireland.

(e) *Compliance Officer*

While PI is not required to appoint a Data Protection Officer (as defined in DP Law), the PI Compliance Officer (the "**Compliance Officer**") is responsible for establishing an appropriate framework within which PI can comply with the provisions of DP Law. The contact details of the Compliance Officer are Éilis Murray, Email: eilis@philanthropy.ie Tel: 01 6768751.

4. **Use of Data Processors by PI**

4.1 In the context of PI's activities, any party Processing the Personal Data on behalf of PI is a Processor for the purposes of DP Law. For example, where PI engages a third party to provide payroll services, that third party service provider is a Processor acting on the instructions of PI.

4.2 In order to comply with DP Law requirements and to ensure that the rights of the Data Subjects are protected, PI must ensure that such Processors provide sufficient guarantee(s) to implement appropriate technical and organisational measures as set out in DP Law. In addition, the Processing must be based on a contract or other written agreement with PI that includes the data protection provisions prescribed in DP Law in order to safeguard the Personal Data of the Data Subjects.

5. T **Types of Personal Data held by Us**

5.1 PI typically retain the following types of Personal Data, usually about clients, directors, and employees:

(a) name, address, phone numbers, email address, date of birth, occupation, bank account details, PPSN (directors and employees only).

5.2 PI does not ordinarily Process Special Categories of Personal Data.

6. **PI's Role as Controller**

6.1 For the purposes of DP Law, PI is a Controller of certain Personal Data relating to clients, directors, and employees. Consequently, PI is responsible for, and must be able to demonstrate compliance with, the data protection principles set out in Article 5 GDPR. These seven principles are summarised as follows:

(a) *Lawfulness, Fairness and Transparency*

Personal Data shall be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

(b) *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;

(c) *Data Minimisation*

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;

(d) *Accuracy*

Personal Data shall be accurate and, where necessary, kept up to date;

(e) *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;

(f) *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; and

(g) *Accountability*

PI, as a Controller, shall be responsible for, and be able to, demonstrate compliance with the GDPR.

6.2 As PI only stores and Processes Personal Data in fulfilment of its business obligations in line with PI's mission, and given the security measures engaged by PI to protect the confidentiality of this Personal Data, PI complies with these principles.

7. What Does PI Do with Personal Data?

7.1 PI Processes Personal Data provided to it only for the purposes of providing services to its members, and promoting philanthropy in Ireland.

7.2 In order for the Processing of Personal Data to be lawful, PI must have a lawful basis for Processing pursuant to Article 6 of the GDPR. The lawful bases on which PI will Process Personal Data will ordinarily be:

(a) *Contractual Necessity*

Article 6(1)(b) GDPR permits Processing that 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;

(b) *Legal Obligation*

Article 6(1)(c) GDPR permits Processing that is necessary for compliance with a legal obligation to which the Controller is subject; and

(c) *Legitimate Interests*

Article 6(1)(f) GDPR permits Processing which 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 or fundamental rights and freedoms of the data subject which require protection of Personal Data.

7.3 Another lawful basis provided for under DP Law is consent. PI does not ordinarily rely on consent to Process Personal Data.

7.4 From time to time, PI may disclose Personal Data relating to third-party Controllers such as payroll service providers. Such third-party Data Controllers will have their own privacy policies in place in respect of Personal Data disclosed. Typically, PI will not disclose Personal Data to third parties unless the Data Subject has consented to this disclosure or unless the disclosure to the third party is required in order to provide PI's services.

7.5 PI may also disclose Personal Data to third parties where required in order to comply with any applicable law, such as a summons, a search warrant, a court or regulatory order, or other statutory requirements.

7.6 By adopting the measures in this Policy, PI strives to ensure that the right balance is struck between PI's obligation to administer its social finance operations, and the rights and interests of individuals whose data may be Processed by PI in relation to that purpose.

8. Transparency

8.1 Pursuant to the GPDR, PI has introduced a new Data Protection Statement to be shared on PI's website **("Data Protection Notice**"). A copy of the template Data Protection Notice is included in Appendix 1. This is intended to ensure that all Data Subjects are aware of the nature of the Processing of Personal Data undertaken by the SLOs and PI as required by DP Law.

9. Retention

9.1 PI will keep Personal Data only for as long as the retention of such Personal Data is deemed necessary for the purposes for which it is Processed. The retention period, or guidelines used to determine the retention period, of Personal Data relating to a particular category of Data Subjects will be specified in the relevant Data Subjects' Data Protection Notice.

10. Data Security and Data Breach

10.1 PI is required to ensure that appropriate technical and organisational measures are in place to protect Personal Data. These measures are designed to protect Personal Data from unlawful or unauthorised destruction, loss, change, disclosure, acquisition or access.

10.2 Personal Data is held securely using a range of security measures including, as appropriate, physical measures such as locked filing cabinets and restricted access to documents on network drives.

10.3 DP Law requires PI, as a Controller, to notify the DPC and affected Data Subjects in the case of certain types of Personal Data Breaches. The notification to the DPC must occur within 72 hours of becoming aware of the Personal Data Breach.

10.4 All Staff are required to report any actual or potential data protection compliance failures to Éilis Murray, CEO in order to allow PI to comply with its reporting obligations under DP Law, if required.

11. Data Subject Rights

11.1 DP Law provides certain rights in favour of Data Subjects ("**Data Subject Rights**"), which allow a Data Subject to make certain requests to PI as a Controller in respect of their Personal Data. The rights in question are as follows:

(a) the right of access to Personal Data (exercised by way of a data subject access request). This enables a Data Subject to receive a copy of the Personal Data PI holds about him / her and to check that we are lawfully Processing it;

(b) the right to rectify any incorrect or incomplete Personal Data;

(c) the right to request erasure of Personal Data (commonly known as the "**right to be forgotten**");

(d) the right to restrict PI's Processing of Personal Data;

(e) the right of data portability. i.e. the right to receive Personal Data in a structured, commonly-used and machine-readable format, and the right to have that Personal Data transmitted to another Data Controller; and

(f) the right to object to the Processing of Personal Data where PI is relying on its legitimate interest (or those of a third party) as its lawful basis for Processing. Data Subjects also have the right to object where we are Processing their Personal Data for direct marketing purposes.

11.2 PI is normally obliged to respond to all Data Subject Rights within one calendar month of receipt. No fee may be charged.

12. Dealing with Data Subject Access Requests

12.1 If a written request is received for access to Personal Data, this should be forwarded to the Éilis Murray, CEO immediately.

12.2 If a request for Personal Data is received by telephone, the caller's identity must be verified. If the caller's identity cannot be verified, Staff should refer the request to Éilis Murray, CEO.

13. Data Transfers outside the EEA" \l1 **Data Transfers outside the EEA**

13.1 Personal Data should not be transferred to a country or territory outside the European Economic Area (the "**EEA**"), unless that country or territory ensures an adequate level of protection for the Processing of Personal Data.

13.2 PI does not currently transfer Personal Data outside of the EEA. If this changes in the future, PI will ensure that Personal Data is not transferred to a country or territory outside the EEA unless appropriate safeguards for the protection of that Personal Data are in place in accordance with DP Law.

14. **Remedies for non-compliance**

14.1 Each Data Subject has the right:

(a) to lodge a complaint with the DPC if the Data Subject considers that PI's Processing of Personal Data infringes DP Law;

(b) to an effective judicial remedy against PI where he or she considers his or her rights under DP Law have been infringed as a result of PI's Processing of Personal Data being non-compliant with DP Law; and

(c) to receive compensation from PI for any material or non-material damage as a result of non-compliance with DP Law.

14.2 The DPC may also impose administrative fines in respect of infringements of DP Law.

15. Amendments

15.1 PI reserves the right to modify this Policy as necessary, for example, to comply with changes in laws or PI's policies and procedures.

15.2 Changes to this Policy will shall be applicable from the effective date of implementation. Notice of material changes will be provided to Staff via email or other internal communications.

16. Governing Law

16.1 This Policy is governed by the laws of Ireland.

17. Contact Details

17.1 Address: Philanthropy Ireland, 56 Fitzwilliam Square Dublin 2.

T: +353 (0)1 676 8751 E: info@philanthropy.ie