TII DATA PROTECTION POLICY

1. Introduction

The purpose of this document ("Policy") is to provide a concise policy statement regarding the data protection obligations of Transparency International Ireland ("TII"), including under domestic law the Data Protection Act 2018 and European law [the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 and the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("relevant legislation").

For the avoidance of doubt, where there is a conflict between domestic law and the General Data Protection Regulation ("GDPR"), the GDPR takes precedence and is directly applicable. All legislative references in this Policy refer to the provisions of the GDPR, unless otherwise stated.

2. Rationale

As a data controller and data processor, TII must comply with the data protection principles set out in the relevant legislation and in particular the GDPR. The Policy applies to the processing of personal data, including sensitive personal data, undertaken by TII in the course of its activities.

3. Scope

The Policy applies equally to all personal data, whether in manual or automated form. All personal data, including special categories of personal data, will be treated with equal care by TII. Unless specifically otherwise stated, all references to personal data in the Policy shall include special categories of personal data.

The Policy should be read in conjunction with the associated Subject Access Request Procedure, Data Retention and Destruction Policy, Record Retention and Destruction Affirmation for Staff Members, Data Loss Notification procedure, Data Sharing/Processing Agreement, Password Policy, Remote Access Policy, Remote Access Connection Agreement, Network Drives, Privacy Notice for Speak Up Callers, Privacy Notice for Website, Template Response for Subject Access Request, Staff and Volunteer Privacy Notice, IAW Members Privacy Notice, Training Participants Privacy Notice, Conference Participants Privacy Notice, TI Ireland Board Members Privacy Notice, Non-Disclosure Agreement (attached as Appendices 1-18 to the Policy).

4. Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within the Policy:

Data	Data means automated data and manual data. "Automated data" means information that— (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose or

	(b) is recorded with the intention that it should be processed by means of such equipment. "Manual data" means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
Data Controller	TII (the natural or legal person or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data)
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of TII (excluding employees and volunteers of TII, processing personal data on behalf of TII Data in the course of his/her employment).
Data Protection Officer	A person appointed by TII to (a) inform and advise TII and its employees/volunteers who carry out processing of their obligations pursuant to the relevant legislation, including the GDPR; (b) monitor compliance with the relevant legislation, including the GDPR, and with the policies of in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) cooperate with the Data Protection Commission; (e) act as the contact point for the Data Protection Commission on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter; (f) deal with Subject Access Requests; (g) deal with personal data breaches. This person is currently Donncha Ó Giobúin (Helpline Coordinator)
Data Subject	An individual who is the subject of Personal Data.
Personal Data	Any information relating to an identified or identifiable living person ('data subject'); an identifiable living 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	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. Data on the commission or alleged commission of any offence by the data subject is defined as sensitive personal data under Irish legislation but not under the GDPR, although it does continue to benefit from special protection under GDPR.

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.
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a manner that specific information relating to a particular individual is readily accessible.

5. TII as Data Controller and Data Processor

In the course of its daily organisational activities, TII determines the purpose and means of processing personal data in relation to:

- Speak Up Helpline callers (including those who contact the service via email, post or visit)
- IAW Members
- IAW training participants
- IAW conference participants
- Job and volunteer/internship applicants
- Employees
- Volunteers
- Third party service providers engaged by TII
- Board members and company members
- Supporters/donors/funders

TII also acts as a data processor for the Transparency Legal Advice Centre ("TLAC").

In accordance with the relevant legislation, this data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. Not all staff members will be expected to be experts in the relevant legislation. However, in compliance with the relevant legislation, TII is committed to ensuring that all staff and volunteers involved in the processing of personal data have sufficient training and awareness of the relevant legislation and the Policy in order to ensure compliance with same and TII's security rules when processing personal data and to be able to anticipate and identify a data protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is immediately informed, in order that appropriate corrective action is taken.

6. Records of Processing Activities

TII shall maintain a written record of personal data processing activities under its responsibility in accordance with Article 30 GDPR. That record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, any joint controllers, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) GDPR.

7. Data Processors (Articles 28-33, 37, 44 & 82-83; Recitals 81-82)

In the course of its role as Data Controller, TII may engage third parties to process Personal Data on its behalf ("Data Processors"). In this regard, TII will only use Data Processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of the GDPR, including for the security of processing. In each case, the processing undertaken by the Data Processor will be governed by a formal, written binding GDPR-compliant contract (Appendix 5) with TII, setting out the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the Data Processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject.

Regular audit trail monitoring will be undertaken by the Data Protection Officer to ensure compliance with the contract.

In order to demonstrate compliance with the GDPR, each Data Processor must maintain records of processing activities under its responsibility and cooperate with the Data Protection Commission and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

8. Subject Access Requests (Articles 12, 15, 23 and Recital 63)

Any formal/written request by a Data Subject to TII for a copy of their personal data (a "Subject Access Request") will be referred, as soon as possible, to the Data Protection Officer, and, if valid, will be processed as soon as possible and within one calendar month at the latest unless an extension of time is required. TII will take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The Data Subject will provide proof of identification/address as a way to ensure that the request is bona fide.

When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Where TII processes a large quantity of information concerning the Data Subject, it shall be able to request that, before the information is delivered, the Data Subject specifies the information to which the request relates.

Where Subject Access Requests are complex or numerous such that an extension of time to respond is required, TII will inform the Data Subject of any such required extension within one month of receipt of the Subject Access Request, together with the reasons for same. In responding to a Subject Access Request, TII will provide the Data Subject with the information stipulated in Article 15(1) GDPR, where applicable.

A Subject Access Request may be refused by TII on the basis that it is manifestly unfounded or excessive, in particular because of its repetitive character. TII will bear the burden of demonstrating the manifestly unfounded or excessive nature of any such request. TII may charge a reasonable fee for any further copies requested by the Data Subject or where requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information. Where TII refuses to respond to a request, it will, without delay and, at the latest, within one calendar month explain in writing why, informing the data subject of his/her right to complain to the Data Protection Commission and to a judicial remedy.

The Data Subject has the following rights:

- A right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her;
- A right to request that any incomplete information be updated such that it is complete;
  A right to request the controller to delete personal data held;
- A right to request that the controller no longer processes their personal data for particular purposes or to object to the controller's processing of their personal data for particular purposes;
- A right to request a copy of personal data in a structured, commonly used machine readable format.

See Appendix 1 for Subject Access Request Procedure and Appendix 12 for a template response.

9. The Data Protection Principles

The following key principles are enshrined in legislation and are fundamental to this policy.

In its capacity as Data Controller, TII ensures that all data shall be:-

9.1 *Processed lawfully, fairly and in a transparent manner (Articles 5(1)(a), Articles 12-14, Recitals 58-62, WP29 Guidance on Transparency)*

In order to comply with this principle, where personal data relating to a data subject are collected from the data subject by TII, TII shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a) the identity and the contact details of TII, being the Data Controller, and, where applicable, TII's representative;
b) the contact details of TII's data protection officer;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) where the processing is necessary for the purposes of the legitimate interests pursued by TII or a third party, the legitimate interests pursued by TII or by a third party and an explanation of those interests;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, the fact that TII intends to transfer personal data to a third country or international organisation, safeguards in place and the means by which to obtain a copy of them;
g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

h) the existence of the right to request from TII 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;
i) where the processing is based on consent or explicit consent for one or more specific purposes, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
j) the right to lodge a complaint with the Data Protection Commission;
k) whether the provision of 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; and
l) 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. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information under the above paragraphs.

TII will take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

TII meets these obligations in the following ways:

- A privacy notice is read to Speak Up callers prior to the collection of their personal data (see Appendix 10). Where an individual contacts the service by email, a notice is sent to them by email. The caller is referred to the helpline privacy policy which is also available on the website.
- During staff and volunteer inductions, Personal Data including copy passport information, address and qualifications is collected with an explanation that this is collected by TII for due diligence, to check identity and competence; and that referees will be contacted to provide references. A Privacy Notice as outlined in Appendix 13 will be read to the staff or volunteer. The Privacy Notice will also cover data not obtained directly from the employee, such as references and management reviews. The Privacy Notice will indicate the categories of data processed; from which source the data originated; and, if applicable, whether it came from publicly accessible sources. The Privacy Notice points out that any Personal Data such as bank details which are collected for the purpose of payment of salary and benefits may be disclosed to the Revenue Commissioners, the Law Society of Ireland and other authorities for purposes of regulatory compliance. This will be included on the Staff/Volunteer Privacy Notice in the Appendix 13.
- In relation to Integrity at Work, a privacy notice will be sent to all existing members as an Addendum to their contract of membership. The data will be processed on the basis that processing is necessary for the performance of the Membership Contract. This will be separate from the main body of the contract. When TII works with IAW Members to provide training, a privacy notice will be appended to the Training Needs Analysis Form and to the Attendee Feedback Form.
- TII will display on its webpages a privacy policy as set out in Appendix 11.
- If TII intends to record activity on CCTV or video, a fair processing notice will be posted in full view.

9.2 ***Processing conditions***

- TII processes Speak Up Helpline callers' personal data on the basis that such processing is necessary for the legitimate interest of TII to process reports obtained by TII, and to refer callers to TLAC, if necessary. TII also relies on its legitimate interest in gathering statistics and reporting on corruption and abuses of power in the workplace, and to support people to promote integrity and stop corruption in all its forms.

- TII processes any special categories of personal data received from Speak Up Helpline callers on the basis of the substantial public interest in preventing corruption and other abuses of power in the workplaces.

- TII processes employee or volunteer personal data on the following grounds:

  - Such processing is necessary for the performance of a contract between TII and its staff (Art 6(1)(b)).

  - In the case of volunteers, such processing is necessary for the legitimate interest of TII (Art 6(1)(f)) to check the identity and competence of volunteers to ensure the quality and consistency in the services provided by TII.

- TII processes board member and company member personal data on the basis that such processing is required to fulfil TII's obligations under the Companies Act 2014 and other relevant legislation.

- TII processes the personal data of IAW Members and their employees on the basis that it is necessary for the performance of the contract between IAW and TII.
- TII will ensure that collection of Personal Data is justified under one of the other processing conditions specified in the legislation, such as that the processing is necessary for complying with a legal obligation or pursuing TII's legitimate interests.
- TII will not process Personal Data in pursuance of its legitimate interests where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the Data Subject.

9.3 ***Collected for specified, explicit and legitimate purposes (Article 5(1)(b))***

Personal data will be collected by TII for specified, explicit and legitimate purposes only, and not further processed in a manner that is incompatible with those purposes. The purposes of the processing for which the personal data is intended as well as the legal basis for the processing will be provided to the Data Subject at the point of collection of the personal data.

9.4 ***Not be further processed in a manner incompatible with the specified purpose(s)***

TII will not further process Personal Data in a manner incompatible with the specified, explicit and legitimate purposes for which it was collected, except to the extent that TII continues to process data in a pseudonymised format for statistical purposes.

9.5 ***Processed in a manner that ensures appropriate security of the personal data, including protection against a personal data breach, using appropriate technical or organisational measures***

TII will employ high standards of security in order to protect the Personal Data under its care. TII's Password Policy (Appendix 6), Data Sharing Confidentiality Agreement (Appendix 5) and Data

Retention & Destruction Policy (Appendix 2) help ensure protection against personal data breaches, including unauthorised or unlawful processing, accidental loss, destruction or damage of any personal data held by TII in its capacity as Data Controller.

Speak-Up Helpline Data

All Speak Up Helpline hard copy data is stored in a locked filing cabinets in locked offices. Access to the filing cabinet is restricted to Helpline Staff and Volunteers. Access to the Speak Up Helpline Database is restricted to those working on the Helpline. Passwords to access to the Database are distributed by the Helpline Co-ordinator. Each Volunteer and Staff Member working on the Helpline signs a non-disclosure document on induction (See Appendix 18). Any remote access to IT systems is governed by the Remote Access Policy (Appendix 7).

The data is processed on the basis that the processing is necessary for the purposes of the legitimate interests pursued by TII of providing support and information to those who wish to speak up about wrongdoing and to compile statistics and general information to monitor demographics and general patterns of corruption and wrongdoing, produce anonymised reports and formulate recommendations to policy-makers as appropriate.

TII may refer a Speak-Up Helpline caller to TLAC for the purposes of obtaining legal advice. With the consent of the caller, TLAC may contact the caller's employer for the purposes of providing a Memorandum of Concern which will provide anonymised feedback to the employer.

To the extent that TII processes special categories of personal data of callers, TII does so on the basis that such processing is necessary for reasons of substantial public interest, that being the prevention of corruption and abuses of power in the workplace (Art 9(2)(g) GDPR) and for the establishment, exercise or defence of legal claims (Art 9(2)(f) GDPR).

TII does not process or control any third party data disclosed by Helpline Callers in emails or on telephone calls.

IAW Member Data

All IAW Member Data is kept on a secure drive. Access is by password and is restricted to IAW personnel. IAW Member Data is shared only with TII Associates who provide training on behalf of IAW. Each Volunteer and Staff Member working on IAW signs a non-disclosure document on induction (See Appendix 18. Any remote access to IT systems is governed by the Remote Access Policy (Appendix 7). The data is processed on the basis that it is necessary for the performance of the contract between IAW and TII.

IAW Member Training Data

All participants in IAW training complete a Training Needs Analysis (TNA) and a feedback form. These contain personal data. The data will be stored in TII's secure IT systems and access is restricted to IAW staff and TII Associates. The TNA will be accompanied by a privacy statement. The training participant will give consent to the processing of the personal data of training participants is necessary for the legitimate purposes of receiving the training and that the training is necessary for the performance of the IAW contract between TII and the IAW Member.

IAW Conference/Forum Participant Data

TII process the personal data of all participants in IAW Forums and Events. All names, addresses, employer details, phone numbers and email addresses are stored in TII's secure IT systems and access

is restricted to IAW staff. The grounds for processing the data is on the basis of the performance of the contract between TII and the IAW Member. For those attending outside the contractual engagement, we will process their data on the basis of their consent, for which they have a right to withdraw at any time by sending us an email. Any emails sent to promote further events will enable participants to request to be removed from the mailing lists and will contain a link to our Privacy Notice on the TII Website.

Volunteer Recruitment Data

All Volunteer Recruitment data is stored on secure IT systems and in hard copy in a locked filing cabinet. Access is restricted to TII's Helpline Co-ordinator. CVs are kept for one year. CVs are not shared with other personnel without the consent of the data subject. On receipt of the application for a position, a privacy notice will be emailed to the applicant volunteer.

Staff Recruitment Data

All recruitment data related to staff is kept on a secure drive on our IT systems and in hard copy in a locked filing cabinet. Access is restricted to Management Staff within the organisation. CVs are kept on file for a year. CV's are not shared with other personnel without the consent of the data subject. On receipt of the application for a position, a privacy notice will be emailed to the applicant volunteer.

Volunteer Data

All volunteer data (CV, Identity Documents, Grade or Degree Certificates and/or transcripts of results, and induction documents) are stored in hard copy in a locked cabinet and on a secure drive on our IT systems. This data is processed for the purposes of completion of the internship with TII. This information is kept on file for 3 years after the departure of the volunteer for the purpose of providing references. Feedback forms and exit interview material is stored on a secure drive on our IT systems. Access is restricted to the relevant line managers. If this material is printed in hard copy it will be shredded after use. This information is retained for 3 years after the departure of the volunteer in case it is required for reference purposes.

Staff Data

All staff data (Employment contract, CV, Identity Documents, Grade or Degree Certificates, induction documents and any health, pensions and payroll data) is stored in hard copy in a locked cabinet. This data is processed for the purposes of the completion of the employment contract. This information is kept on file for 6 years after the departure of the staff for the purpose of providing references. Feedback forms and exit interview material is stored on a secure drive on our IT systems. Access is restricted to Management. If this material is printed in hard copy it will be shredded after use. This data is processed for the purposes of the execution of the employment contract and any legal obligations arising after the departure of the staff member.

Board Members Data

All data pertaining to Board Members (identity, Directorships, qualifications and CVs) is stored on a secure cloud-based drive. This data is processed for the purposes of the completion of the term of Office for the Directorship and is necessary for compliance with TII's legal obligations under the Companies Act 2014.This information is kept on file for three years after the departure of the Board Member. Access is restricted to Management. If this material is printed in hard copy it will be shredded after use.

Updated: 28 May 2019

Board Data

The minutes of Board meetings where the list of attendees is included is personal data. The minutes of the Board Meetings are saved on secure server with access limited to the CEO and Office Administrator. Any information relating to funders/donors or other members of the company are handled in the same way.

9.6 ***Be kept accurate and, where necessary, up-to-date***

Speak Up Helpline Data

When a caller contacts the Speak Up helpline, a hard copy form must be filled out during the call by the call handler. A summary must be read back to the caller and the database updated immediately afterwards, to ensure a high level of accuracy. Where there is further contact with a client, any updated information must be recorded accurately and promptly in hard copy and electronic form. The data held will be reviewed by the Speak Up Helpline Co-ordinator, who will file all necessary consents with the data, diarise data retention/destruction periods, and deal with any subject access requests.

IAW Member Data

This will be kept accurate and up-to-date on an ongoing basis. The nature of the programme means that data is exchanged on an ongoing basis. The IAW Programme Manager and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

IAW Member Training Data

This will be kept accurate and up-to-date on an ongoing basis. Training is provided regularly, meaning that data is exchanged regularly. The IAW Programme Manager and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

IAW Conference/Forum Participant Data

This will be kept accurate and up-to-date on an ongoing basis. The IAW Programme Manager and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

Volunteer Recruitment

This will be kept accurate and up-to-date by the Helpline Co-ordinator and the Data Protection Officer. The Helpline Manager will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

Staff Recruitment

This will be kept accurate and up-to-date by the Office Administrator. The Office Administrator and the Data Protection Officer will review and amend the data when notified of a change, will file all

necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

Volunteer Data

This will be kept accurate and up-to-date by the Helpline Co-ordinator. The Helpline Manager and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

Staff Data

This will be kept accurate and up-to-date by the Office Administrator. The Office Administrator and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

Board Members Data

This will be kept accurate and up-to-date by the Office Administrator. The Office Administrator and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

Board Data

This will be kept accurate and up-to-date by the Office Administrator. The Office Administrator and the Data Protection Officer will review and amend the data when notified of a change, will file all necessary consents for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

TII's Data Protection Officer will:

- conduct a review of sample client data every six months to ensure accuracy;
- review and update staff contact details and details of next-of-kin every two years.

9.7 ***Be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (Data Minimisation)***

Records should contain all relevant facts and be created at the time of the action or transaction or as soon as possible afterwards by a person authorised to carry out that function, action or transaction. Once created, additions or annotations to the record can only be carried out by those authorised to do so and any amendment should be explicitly indicated on the record.

TII will ensure that the Personal Data it processes is relevant to the purposes for which those data are collected. Personal Data which is not relevant to such processing will not be acquired or maintained.

9.8 ***Not be kept in a form which permits identification of data subjects for longer than is necessary for the specified purposes for which the personal data are processed.***

TII has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format. Further details can found in Appendix 2 to this policy.

Once the respective retention period has elapsed, TII undertakes to destroy, erase or otherwise put this Personal Data beyond use.

9.9 Be managed and stored in a form which, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them

TII will ensure that Personal Data is filed correctly, in clearly labelled folders (electronic and manual). In particular, the Helpline Manager is to carry out spot checks on the Speak Up client database to ensure that volunteers are recording Speak Up Personal Data correctly.

The Helpline Manager is responsible for the correct filing and diarising of destruction dates for data relating to Volunteer Recruitment and those Volunteers who participate in an internship with TII.

The IAW Programme Manager is responsible for the management and storage of data in relation to all IAW Members, participants in training programme and other conferences and events.

The Office Manager/CEO is responsible for the management and storage of personal data in relation to staff and for diarising destruction dates for data relating to Staff Recruitment and Employees.

10. Business contacts

Direct marketing rules must be consulted before contacting individuals at organisations for the purposes of promoting TII's activities.

11. Implementation

Failure of TII's staff to process Personal Data in compliance with the Policy, including the Appendices to the Policy, may result in disciplinary proceedings.

APPENDIX 1: SUBJECT ACCESS REQUEST PROCEDURE

Articles 12, 15 and 23 and Recital 63

To obtain a copy of your personal data as held by Transparency International Ireland ("TII"), you will need to submit a written request, to the Data Protection Officer, Transparency International Ireland, Floor 3, 69 Middle Abbey Street, Dublin 1.

In order that TII can sufficiently satisfy itself as to your identity before providing you your personal data, please enclose proof of identity, such as a copy driving licence or passport, with your request.

If TII processes a large quantity of information concerning you, please specify in your request the information you require.

TII will respond as quickly as possible to your request and, at the latest, within one calendar month of receipt of your valid request, unless an extension of time is required. Where your request is complex or numerous, TII may require an extension up to a maximum of two further months to respond to your request. If so, TII will inform you in writing of any such required extension within one month of receipt of your request, together with the reasons for the extension.

If requested by you, your personal data may be provided to you orally, provided that TII is satisfied as to your identity.

In responding to a Subject Access Request, TII will provide the Data Subject with the following information, where applicable:

- The purposes of the processing;
- The categories of personal data;
- The recipients or categories of recipients;
- The data retention period or criteria used to determine that period;
- The individual's rights including: the right to rectification, erasure; restriction or objection to the processing;
- The right to complain to the Data Protection Commission;
- The source of the information if not collected directly from the data subject;
- Details of any automated processing, including profiling; the logic involved, and the significance and envisaged consequences of the processing for the data subject; and
- Where data are transferred out of the EEA, the appropriate safeguards in place.

Where a request is manifestly unfounded or excessive, TII may either refuse to take any action on your request or charge a reasonable fee for the administrative costs of providing the information. If your request is refused, TII will inform you without delay and, at the latest, within one month of receipt of your request, of the reasons for not taking action on your request and of the possibility to lodge a complaint with the Data Protection Commission and/or seek a judicial remedy.

Please note that personal data can be withheld under certain circumstances, as set out in Section 60 of the Data Protection Act 2018.

APPENDIX 2: DATA RETENTION AND DESTRUCTION POLICY

The purpose of this Data Retention and Destruction Policy is to ensure that TII ("TII") controls and processes personal data in accordance with the requirements of all applicable data protection laws, including the GDPR, and to ensure that official records no longer needed by TII are securely destroyed at the proper time.

This policy applies to all personal data controlled and processed by TII in the course of its operations, including but not limited to:

- typed, or printed hardcopy (i.e., paper) documents;
- electronic records and documents (e.g., email, Web files, text files, PDF files);
- video or digital images;
- graphic representations;
- records on storage devices;
- electronically stored information contained on network servers and/or document management systems; and
- recorded audio material (e.g., voicemail)

This document is intended to be read along with the Data Protection Policy to which this document is appended.

All employees responsible for the retention of records are also responsible for the proper destruction of records following the stated retention period (see table below). Manual records must be destroyed by shredding or other means as appropriate to ensure that all sensitive or confidential material can no longer be read or interpreted.

1. Administration

a. Record Retention Schedule.

Attached to this policy is a Record Retention Schedule (Attachment A) that is approved as the maintenance, retention and disposal schedule for records of TII.

b. Authority and responsibility of the Data Protection Officer

The Data Protection Officer shall be authorised to: (a) review and make modifications to the Record Retention Schedule from time to time to ensure that this Policy complies with Data Protection laws, including the GDPR, and includes the appropriate document and record categories for TII; (b) monitor the compliance of TII employees and volunteers with this Policy; and (c) take such other action as may be authorised by TII's Board of Directors.

c. Distribution of policy to staff members and volunteers

The Data Protection Officer will arrange for every employee and volunteer to receive a copy of this Policy and each such individual shall sign a statement (Attachment B) that affirms that he or she has received a copy of this Policy, has read and understands it, and has agreed to comply with it. There will be a training for staff as part of the roll-out of the Policy.

2. Document destruction procedures

Following the expiration of the applicable period set forth in the Record Retention Schedule, the Personal Data should be prepared for destruction in the manner prescribed by the Data Protection Officer, unless the Data Protection Officer in consultation with the Board of Directors has suspended the destruction of any Personal Data for reasons of litigation or audit.

3. Suspension of record disposal in event of litigation or claims

In the event any employee of TII reasonably anticipates or becomes aware of an audit or the commencement of any litigation against or concerning TII, such employee shall inform the Data Protection Officer and any further destruction of personal data shall be suspended until such time as the Data Protection Officer determines otherwise. The Data Protection Officer shall take such steps as are necessary to promptly inform affected staff of any suspension in the destruction of documents.

All paper documents destroyed pursuant to this policy shall be cross-cut by mechanical shredder. Electronic data contained on servers and hard drives shall be deleted and overwritten, under the supervision of the Data Protection Officer. Electronic data contained on all other media shall be destroyed by the physical destruction of that media.

4. Record retention schedule

This Record Retention Schedule sets forth a schedule of retention periods for key Personal Data. This is further recorded on TII's Article 30 Compliance Statement.

If you have questions about the retention or destruction of specific documents or the data types they contain, please contact the Data Protection Officer.

	Type of Data/Record	Retention Period	Personnel Responsible
SU Helpline Data	Call Record Forms (paper)	Six years, legal limitation expiry	Helpline Co-ordinator
	ALAC database entry (electronic)	Six years, legal limitation expiry	Helpline Co-ordinator
IAW Member Data	Contract with Member (paper/electronic)	Six years from expiry of Contract	IAW Programme Manager
	Records of Meetings (paper/electronic)	Six years from expiry of Contract	IAW Programme Manager
	All correspondence (email/letter)	Six years from expiry of Contract	IAW Programme Manager
IAW Member Training Data	List of Attendees (paper/electronic)	Six years from date of training	IAW Programme Manager
	Correspondence	Six years from date of training	IAW Programme Manager
	TNA from each participant	Six years	IAW Programme Manager
	Feedback forms	Six years	IAW Programme Manager
IAW Conference/Forum Data	List of Attendees	Six years	IAW Programme Manager
	Correspondence	Six years	IAW Programme Manager
Volunteer Recruitment	CV/email/correspondence	1 year after recruitment concluded (limitation for Equality Act claim)	Helpline Co-ordinator
Staff Recruitment	CV/email/correspondence	1 year after recruitment concluded (limitation for Equality Act claim)	Office Co-ordinator/CEO
Volunteer Records	Identity/Qualifications/Bank Details/Health Information/Travel data/Expense forms/Feedback forms/Exit interviews	3 years after end of internship for purpose of references	Helpline Co-ordinator
Staff Records	Identity/Qualifications/Contract/Bank Details/Health Information/Pension Payments/Travel data/Expense forms/Financial Records/Tax Records/Income Records	6 years after termination of employment; with the exception of references, pension and benefit records – these should be kept permanently	Office Co-ordinator/CEO
Board Member Data	Identity/Qualifications/Bank details	3 years after the end of the Directorship	Office Co-ordinator/CEO

Board Data	Board of Directors' records including minutes of meetings	Indefinitely while the company is still in operation and 6 years after	Office Co-ordinator/CEO
	Bank information/email addresses on funders/donors/other supporters	Indefinitely to the extent that this information is retained in historical email inboxes	Office Co-ordinator/CEO

APPENDIX 3: RECORD RETENTION AND DESTRUCTION AFFIRMATION

AFFIRMATION STATEMENT

I, _____, have read and understand the foregoing

Record Retention and Destruction Policy of Transparency International Ireland and hereby agree to comply with same.

_____

Name of Worker/volunteer/contractor

_____

Title

_____

Date

APPENDIX 4: DATA LOSS NOTIFICATION PROCEDURE

Articles 33, 34 and Recitals 76, 85-88 and WP 29 Guidance on Breach Notification

1. Introduction

The purpose of this document is to provide a concise procedure to be followed in the event that Transparency International Ireland ("TII") becomes aware of a personal data breach. The procedure takes account of legal obligations under domestic and EU law and is consistent with the guidelines issued by the Data Protection Commission in 2011.

2. Rationale

The response to any personal data breach can have a serious impact on TII's reputation and the extent to which the public perceives TII as trustworthy.

The consequential impact on our brand can be immeasurable. Therefore, exceptional care must be taken when responding to personal data breaches.

3. Scope

The policy covers both personal and special category personal data controlled and processed by TII. The policy applies all personal data, whether in manual or automated form. All Personal Data will be treated with equal care by TII.

This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request procedure and the Data Retention and Destruction Policy.

4. What constitutes a breach, potential or actual?

A personal data breach is defined as 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.

This could include:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on PCs and applications
- Emailing a list of people/records in error or emailing multiple recipients and revealing their email addresses
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises Personal Data

5. What happens if a breach occurs?

Actual, suspected or potential breaches should be reported immediately to TI Ireland's Data Protection Officer ("DPO").

> *Any employee who becomes aware of a likely data breach and fails to notify the DPO will be subject to TII's disciplinary procedure.*

Updated: 28 May 2019

6. When will the Data Protection Commission be informed?

In cases of a personal data breach, TII shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commission, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Data Protection Commission is not made within 72 hours, it shall be accompanied by reasons for the delay.

A team comprising the DPO and CEO and the staff members implicated in the breach will be established to assess the breach and determine its severity, in particular whether it is likely to result in a risk to the rights and freedoms of natural persons.

The notification to the Data Protection Commission shall at least: (a) describe 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) communicate the name and contact details of the data protection officer or other relevant contact; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by TII to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide the information at the same time, the information will be provided as soon as it is to hand and without undue further delay.

TII shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Data Protection Commission to verify TII's compliance with its breach notification obligations.

7. When will the Data Subject be informed?

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, TII shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the following information:

a) the name and contact details of the data protection officer or other relevant contact point;
b) describe the likely consequences of the personal data breach;
c) describe the measures taken or proposed to be taken by TII to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met: (a) TII has implemented appropriate technical and organisational protection measures, and 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) TII 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.

8. Personal Data Breach logging

TII shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Data

Protection Commission to verify TII's compliance with its breach notification obligations. Such records will be provided to the Data Protection Commission upon request.

Updated: 28 May 2019

APPENDIX 5: DATA SHARING/PROCESSING AGREEMENT

(as per Articles 28-33, 37, 44, 82-83, recitals 81-82)

Transparency International Ireland ("TII") has agreed to make available [define information and type of Personal Data to be shared and categories of data subjects] ("Personal Data") to [name of third partyorganisation/agency] for the sole purpose of [define purpose] [in [location]] on [date]("Agreement").

[Duration of agreement]

TII remains the Data Controller for the purposes of the Data Protection Act 2018 and other applicable legislation, including the General Data Protection Regulation (Regulation (EU) 2016/679).

The Personal Data will be used only [specify the number of times the database/distribution/mailing list will be used by the Third Party, as appropriate; or the instructions for use] by [Third Party Organisation/Agency] for this purpose and not used again[, even for promotion for the same [Event]].

[Third Party Organisation/Agency] will process the Personal Data only on the basis of the authorisation and documented instructions received from TII. The Personal Data may not be used by [Third Party Organisation/Agency] for its own purposes. [Third Party Organisation/Agency] commits itself to maintaining confidentiality of the Personal Data, the Personal Data will not ever be made available by [Third Party Organisation/Agency] to any third party.

[Third Party Organisation/Agency] shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of the individuals the subject of the Personal Data ("Data Subjects") in line with the requirements of Article 32 GDPR.

[Third Party Organisation/Agency] shall take steps to ensure that any natural person acting under the authority of the [Third Party Organisation/Agency] who has access to personal data does not process them except on instructions from TII.

[Third Party Organisation/Agency] shall not engage another processor without prior specific or general written authorisation of TII. In the case of general written authorisation, [Third Party Organisation/Agency] shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving TII the opportunity to object to such changes.

Where [Third Party Organisation/Agency] engages another processor for carrying out specific processing activities on behalf of TII, the same data protection obligations as set out in this binding agreement shall be imposed on that other processor by way of a written contract, in particular sufficient guarantees to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of the Data Subjects. Where that other processor fails to fulfil its data protection obligations, [Third Party Organisation/Agency] shall remain fully liable to TII for the performance of that other processor's obligations.

[Third Party Organisation/Agency] shall maintain a written record of all categories of processing activities carried out on behalf of TII, containing: (a) the name and contact details of the [Third Party Organisation/Agency] and of TII on behalf of [Third Party Organisation/Agency] which is acting, and the data protection officer; (b) the categories of processing carried out on behalf of TII; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in this agreement ("records").

[Third Party Organisation/Agency] shall cooperate with the Data Protection Commission and make the records, on request, available to it, so that it might serve for monitoring the processing operations the subject of the Agreement.

[Third Party Organisation/Agency] shall assist TII by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of TII's obligation to respond to requests for exercising the data subject's rights.

[Third Party Organisation/Agency] shall notify TII without undue delay after becoming aware of a personal data breach, and take all reasonable steps in assisting TII with their obligation to report the breach to the Data Protection Commission. [Third Party/Organisation] also undertakes to take all reasonable steps to assist TII in discharging their obligation to notify data subjects of breaches and carrying out assessments as to the impact of the data breach

[Third Party Organisation/Agency] must register with the Data Protection Commission for the duration of this agreement.

Upon termination or expiry of this agreement, [Third Party Organisation/Agency] must return [or delete] the Personal Data to TII [consider specifying a time limit], and delete existing copies of the Personal Data [unless Union or Member State law requires storage of the Personal Data].

[Third Party Organisation/Agency] shall make available to TII all information necessary to demonstrate compliance with the obligations laid down in the Agreement and shall allow for and contribute to audits, including inspections, conducted by TII or another auditor mandated by TII. [Third Party Organisation/Agency] shall immediately inform TII if, in its opinion, an instruction infringes EU or Member State data protection provisions.

TII will forward the Personal Data to [name of Third Party Organisation/Agency] upon receipt of a signed copy of this agreement.

For the purposes of this Agreement, TII's Data Protection Officer will be designated for both organisations.

[name of Third Party Organisation/Agency] will not make any transfers of personal data to third countries or international organisations without the prior approval of TII.

In the event of the imposition of an administrative fine for non-compliance with data protection rules, [name of Third Party Organisation/Agency] will be fully liable for any breaches caused by its operations.

Parties to this agreement:

_____ Date: _____

Name

[Role], Transparency International Ireland

_____ Date: _____

Name

[Role], [Third Party Organisation/Agency]

Updated: 28 May 2019

APPENDIX 6: PASSWORD POLICY

1. Overview

Strong passwords are critical to computer security. They are the first line of defence for user accounts. A poorly chosen password (easy to guess) or one left in open view could cause the entire network to be compromised or may result in unauthorised access and/or exploitation of TII files.

All staff, including IT contractors or vendors with access to TII systems, and volunteers are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

TII's Data Protection Officer will review, test, assess and evaluate the effectiveness of all technical and organisational measures every six months to ensure that the level of security of processing is appropriate to the risk. The reviews will be documented and records kept to demonstrate compliance.

2. Purpose

The purpose of this policy is to present best practice for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any TII facility, has access to TII network, or stores any non-public TII information.

4. Policy

4.1 General

Users must note that passwords are for their own personal use and must not be shared or disclosed to anyone. It is an offence under the Computer Misuse Act 1990 to access or attempt to gain access to a computer system or computer material to which one is not entitled.

In addition, it is a breach of this policy for any staff to misuse their own or other user's password. If any such misuse results in a staff knowingly elevating their system privileges above those that they have been authorised to use then this will be considered an act of gross misconduct.

- Remote access must not be attempted from insecure locations e.g. open access cluster systems or public terminals.
- All system-level passwords must be changed on at least a bi-yearly basis by TI Ireland's third-party IT Company.
- All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every six months.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

4.2.1. General Password Construction Guidelines

All members of staff and volunteers at TII should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least fifteen alphanumeric characters.
- Contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

Weak passwords have the following characteristics**:**

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, child(ren), car, hometown, favourite food, favourite car or sports club, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "TII” or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variations.

(NOTE: Do not use either of these examples as passwords!)

If you’re unsure about whether your password is good enough, run it through Microsoft’s free password checker. Never use a password rated less than “Strong.”

4.2.2 Password Protection Standards

- Always use different passwords for TII accounts from other non TII access.
- Always use different passwords for various TII access needs whenever possible.
- Do not share TII passwords with anyone, including suppliers, external trainers or sponsors. All passwords are to be treated as sensitive and confidential information.
- Passwords should never be written down, listed on a paper, printed and pasted on a wall, computer desktop, or anywhere around a workstation or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.

Updated: 28 May 2019

- Do not hint at the format of a password (e.g., "my family name") .
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the Data Protection Officer.
- Always decline (select No) the use of the "Remember Password" feature of any applications (e.g., websites, Eudora, Outlook, Netscape Messenger).
- Do not re-use old passwords.

If an account or password compromise is suspected, report the incident to the CEO who will immediately arrange for necessary changes.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by management.

Password cracking or guessing may be performed on a periodic or random basis by TI Ireland's third-party IT company. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

6. Password storage

A single folder containing passwords for every webpage or applications both at system and user-levels is to be encrypted.

APPENDIX 7: REMOTE ACCESS POLICY

1. Overview

Consistent standards for network access are critical to Transparency International Ireland ("TII")'s information security. Any staff member accessing TII's computer systems has the ability to affect the security of others. An appropriate Remote Access Policy reduces risk of a security incident.

2. Purpose

The purpose of this policy is to define secure standards for connecting to TII network from a desktop computer, laptop or any device located outside TII's network.

This policy is mandatory for all staff members of TII and, by accessing any Information Technology ("IT") resources which are owned or leased by TII, staff members are agreeing to abide by the terms of this policy.

3. Scope

The scope of this policy includes all staff members who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to staff members, but also to guests, contractors or any authorised third party commercial service providers who are contracted by TII to provide goods and services (for example: technical support, consultancy etc) and who require access to TII network from a remote location.

Third-party access to the company's externally-reachable systems, such as www.speakup.ie or public web applications such as Mailchimp and SurveyMonkey, are specifically excluded from this policy.

4. Policy

4.1 Principles of Remote Access

Remote access connections must be strictly controlled and only granted to staff members who meet at least one of the following criteria:

- Staff members who make a formal request.
- Staff members approved to work from home or remotely from the office from time to time.
- Third party commercial service providers who are contracted by TII to provide goods and services (for example: technical support, consultancy etc.)

Remote access requests from staff must be reviewed and approved by their line manager to ensure the employee meets the appropriate criteria (as above). Staff must only be granted access to network facilities, drives, services and information systems which are necessary for the employee to carry out the responsibilities of their role or function. See Appendix 9 for list of drives and levels of access.

Third party commercial service provider access requests must be approved and granted by the Data Protection Officer.

Remote access connections must only be used for approved business purposes. Access connection must be used in a lawful and ethical manner at all times.

Each staff member must ensure that the remote access log in details assigned to them are kept confidential at all times and never be shared with others.

Each staff member must respect and protect the privacy and confidentiality of the information they process at all times.

In addition to each user's responsibilities, line managers are directly responsible for:

- The implementation of this policy, as they will be approving remote access requests and supervising the signing of the Remote Access Connection Agreement (see Appendix 9).
- Ensuring that staff members who report to them are made aware of and are instructed to comply with this policy.

4.2 Remote Access Computer Devices

- Any computer connecting to TII network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users should update their antivirus software, as well as other critical software, to the latest versions before accessing the network.
- Only staff members' personal computer devices must be connected to TII network remotely. Computer devices in cafes or other public places must not be connected to TII network remotely.

4.3 Enforcement

This policy will be enforced by management. TII reserves the right to take such action as it deems appropriate against staff members who breach the conditions of this policy.

Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, TII will report such activities to the appropriate authorities.

4.4 Review and Update

This policy will be reviewed and updated every 3 years or more frequently if necessary, to ensure that any changes to TII's organisation structure and business practices are properly reflected in the policy.

4.5 Definitions

Antivirus Software:

An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Remote Access:

Any Connection to TII network(s) or information systems that originates from a computer or device located outside of TII's premises

TII Network:

The data communication system that interconnects TII Local Area Networks (LAN) and Wide Area Networks (WAN).

Third Party Commercial Service Provider:

Any individual or commercial company that have been contracted by TII to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services etc.) to TII.

APPENDIX 8: REMOTE ACCESS CONNECTION AGREEMENT

This form is to be completed for each user who requires remote connection to Transparency International Ireland ("TII")'s electronic servers and systems. The form must be completed and signed by the user and line manager.

AFFIRMATION STATEMENT

I, _____, have read and understand the foregoing

Remote Access Policy of TII and hereby agree to comply with same.

_____

Name of employee

_____

Title

_____

Date

APPENDIX 9: NETWORK DRIVES

1. **TII**

   Organisational files. Access restricted to relevant staff and volunteers.

2. **Speak Up database**

   Accessible to the Speak Up Helpline Co-ordinator and volunteers.

APPENDIX 10: PRIVACY NOTICE FOR SPEAK UP CALLERS

Article 12 and 13 of GDPR

1. Privacy notice – read out on the phone

Before we begin, let me briefly tell you that any information you provide us with will be treated in strict confidence. I would ask you not to identify the specific names of any person/place/product/workplace or organisation related to your concern. General information is enough. This is to avoid compromising yourself or our organisation. If you do provide us with specific information, we may be legally obliged to report it.

I will take notes of the call, which will be stored in hard copy and in electronic form on our secure database and IT systems. We use the information to assess your call and help identify what type of assistance we may be able to provide to you. We also use statistics and general information from this database to monitor patterns, produce reports and formulate recommendations as appropriate. We process any personal data we collect from you in accordance with our legitimate interest, to support people to stop corruption and other abuses of power in the workplace. To the extent that we process any special categories of personal data, we do so on the basis that it is necessary for reasons of substantial public interest.

We may transfer information regarding your case to the Transparency Legal Advice Centre, if you consent to us doing so, for the purposes of facilitating you obtaining legal advice.

This call should not last longer than 15 minutes. I will be taking you through some questions. If you do not want to answer a particular questions, that is fine, please just let me know. The full name of our organisation is Transparency International Ireland limited, and you have a right to request a copy of any personal information we hold about you and to ask for it to be corrected if inaccurate.

You can learn more about our privacy policy on our website at transparency.ie/helpline/privacy

Is all of that OK?

2. Privacy notice – automated email response

General information

Please be aware in all correspondence, that you should take care not to reveal the specific names of any person/place/product/workplace or organisation related to your concern. General information is enough. This is to avoid compromising yourself or our organisation. If you do provide us with specific information, we may need to report it to the relevant authorities if the information incurs a mandatory reporting obligation under Irish Law. TII is required to report instances of potential criminal offences committed against minors or vulnerable adults to Tusla, An Garda Síochána and other relevant authorities. TII is required to report any information it holds that may be relevant to the investigation of a relevant offence pursuant to Section 19 of the Criminal Justice Act 2011.

Privacy notice

Please note that we have logged your concern onto our secure database and IT systems. We use this information (which we also store on hard copy) to assess your case and help identify what type of assistance we may be able to provide to you. We also use statistics and general information from this database to monitor patterns, produce reports and formulate recommendations as appropriate.

The full name of our organisation is Transparency International Ireland Limited and you have a right to request a copy of any personal information we hold about you and to ask for it to be corrected if it is inaccurate.

You can learn more about our privacy policy on our website at https://transparency.ie/helpline/privacy

3. Helpline Privacy notice on our website

In order to provide our services to you, we need to process certain personal data that you provide to us.

Our legal basis for processing your data is in pursuit of our legitimate interests in seeking to support people to promote integrity and stop corruption in all its forms. To the extent that we process any special categories of personal data, we do so on the basis that it is necessary for reasons of substantial public interest, to stop corruption and other abuses of power in the workplace.

We will process your personal data in order to provide you with our services, to assess your call to the Speak Up Helpline and to help identify what type of assistance we can provide to you. We use statistics and general information from all the calls we receive to monitor patterns in corruption and wrongdoing, produce reports and formulate recommendations to policy-makers as appropriate.

We hold your data in hard copy and electronic form. The hard copy data is stored in our secure filing systems at our offices at 69 Middle Abbey Street, Dublin 1. This data is also held on a secure database hosted by the Transparency International Secretariat in Berlin. No-one except our Helpline staff and volunteers have access to the database.

You have a right to request a copy of any personal information we hold about you and to ask for it to be corrected if inaccurate and completed if incomplete. You can ask us to delete personal data that we hold about you. You can object to the processing of your data for certain purposes or request that we no longer process your personal data for a particular purpose. If you make a request for access to your personal data, that data should be provided to you in a structured, commonly used and machine readable format.

We envisage storing your data for a period of six years. Personal data older than this period is pseudonymised, and we will continue to store and process this data for statistical purposes. The Helpline Coordinator is the only person who can decode personal data that has been pseudonymised.

The full name of our company is Transparency International Ireland Limited and we are located at 69 Middle Abbey Street, Dublin 1.

Our data protection officer is Donncha Ó Giobúin and he can be contacted at: helpline@transparency.ie or on 01 554 3938. You can address any queries or complaints in connection with our processing of your data directly to him.

You also have the right to lodge a complaint with the Data Protection Commission. Information can be found on the dataprotection.ie website.

APPENDIX 11: PRIVACY NOTICE FOR WEBSITE

We Respect Your Privacy

This Privacy Policy governs all pages on the TI Ireland website, www.transparency.ie. It does not apply to pages hosted by other organisations, including the websites of other TI National Chapters or related organisations or third party sites. The TI Ireland website may be linked to the websites of such other parties but those other sites may have their own privacy policy which applies to them.

Our website may be used without entering personal information. Different rules may apply to certain services on the Website, however, and are explained separately below. Where we do collect personal information from you (e.g. name, address, email address, telephone number, etc.) it will be in accordance with the provisions of the Data Protection Acts and the General Data Protection Regulation ("GDPR").

Information is considered personal if it can be associated exclusively to a specific natural person. The provisions below serve to provide information as to the manner, extent and purpose for collecting, using and processing personal information by the provider.

TI Ireland process your personal data for the purposes of our legitimate interests in raising public awareness of the work we do and the services we provide to empower people with the support they need to promote integrity and stop corruption in all its forms. Our website is an important part of our strategy to enhance public awareness of the supports and services we provide. TI Ireland will not process personal data where this is unwarranted in any particular case by reason of prejudice to your fundamental rights and freedoms or legitimate interests.

In other circumstances, such as for the use of cookies and subscription to our newsletter, TI Ireland also rely on your consent for the processing of your personal data. When we process your personal data on the basis of your consent, you are free to withdraw your consent at any time. TI Ireland always include an unsubscribe button in our communications, so you can opt out of receiving such communications at any time. You can also withdraw your consent by contacting us using the contact details at the bottom of the page. Please note that if you withdraw your consent, we may not be able to continue providing you with the service to which the consent related.

TI Ireland will not retain your data for longer than is necessary for the purposes of our legitimate interests. To determine the appropriate retention period, we consider the amount, nature and sensitivity of the personal data, the purposes for which we process it and whether we can achieve those purposes through other means.

When we no longer need your personal data, or when consent is withdrawn, we will securely delete or destroy it. We will also consider if and how we can minimise over time the personal data that we use, and if we can anonymise your personal data so that it can no longer be associated with you or identify you, in which case we may use that information without further notice to you.

Please be aware that data transfer via the internet is subject to security risks and, therefore, complete protection against third-party access to transferred data cannot be ensured.

YOUR RIGHTS

Under certain circumstances, by law you have the right to:

Request information about whether we hold personal information about you, and, if so, what that information is and why we are holding/using it.

Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

Withdraw consent. In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. If you wish to exercise any of these rights or have any questions about this policy, please contact:

The Data Protection Officer
Transparency International Ireland
Floor 2
69 Middle Abbey Street
Dublin 1
Ireland

or please email us: helpline@transparency.ie

If you have any concerns over the use of your personal data by TI Ireland, you can submit a complaint to the Data Protection Commission:

Data Protection Commission

21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

Ireland

Phone: +353 (0761) 104 800 | LoCall 1890 25 22 31

Email: info@dataprotection.ie

COOKIES

The TI Ireland Website makes use of so-called cookies in order to recognize repeat use of the Website by the same user/internet connection subscriber. Cookies are small text files that your internet browser downloads and stores on your computer. They are used to improve the Website and services. In most cases these are so-called "session cookies" that are deleted once you leave the Website.

To an extent, however, these cookies also pass along information used to automatically recognize you. Recognition occurs through an IP address saved to the cookies. The information thereby obtained is used to improve our services and to expedite your access to the website.

You can prevent cookies from being installed by adjusting the settings on your browser software accordingly. You should be aware, however, that by doing so you may not be able to make full use of all the functions of the website.

Further information on cookies can be found at:
http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

SERVER DATA

For technical reasons, data such as the following, which your internet browser transmits to us or to our web space provider (so called server log files), is collected: - type and version of the browser you use - operating system – websites that linked you to our site (referrer URL) – websites that you visit - date and time of your visit. This anonymous data is stored separately from any personal information you may have provided, thereby making it impossible to connect it to any particular person. The data is used for statistical purposes in order to improve the Website and services.

CONTACTING US

On the TI Ireland Website we offer you the opportunity to contact us, either by email and/or by using a contact form. In such event, information provided by the user is stored for the purpose of facilitating communications with the user. No data is transferred to third parties. Nor is any of this information matched to any information that may be collected by other components of the Website.

USE OF GOOGLE ANALYTICS WITH ANONYMISATION

The TI Ireland Website uses Google Analytics, a web analysis service from Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA, hereinafter referred to as “Google“. Google Analytics employs so-called “cookies“, text files that are stored to your computer in order to facilitate an analysis of your use of the site.

The information generated by these cookies, such as time, place and frequency of your visits to our site, including your IP address, is transmitted to Google’s location in the US and stored there.

We use Google Analytics with an IP anonymization feature on the Website. In doing so, Google abbreviates and thereby anonymizes your IP address before transferring it from member states of the European Union or signatory states to the Agreement on the European Economic Area.

Google will use this information to evaluate your usage of our site, to compile reports on website activity for us, and to provide other services related to website- and internet usage. Google may also transfer this information to third parties if this is required by law or to the extent this data is processed by third parties on Google´s behalf.

Google states that it will in never associate your IP address with other data held by Google. You can prevent cookies from being installed by adjusting the settings on your browser software accordingly. You should be aware, however, that by doing so you may not be able to make full use of all the functions of the Website.

Google also offers a disabling option for the most common browsers, thus providing you with greater control over the data which is collected and processed by Google. If you enable this option, no information regarding your website visit is transmitted to Google Analytics. However, the activation does not prevent the transmission of information to us or to any other web analytics services we may use. For more information about the disabling option provided by Google, and how to enable this option, visit https://tools.google.com/dlpage/gaoptout?hl=en

USE OF ADDTHIS

We use AddThis to provide buttons on all pages to help you share our content. AddThis is a service from AddThis Inc, 1595 Spring Hill Rd, Suite 300, Vienna, VA 22182, United States.

Your personal data will be sent to a server operated by AddThis Inc. in the United States. For more information on how to opt-out of these cookies view the AddThis privacy policy here: http://www.addthis.com/privacy/privacy-policy

AddThis may – without limitation – use the following Usage Data:

Internet Protocol (IP) address, Mobile Advertising ID (MAID) (which allows mobile app developers to identify who is using their mobile apps), mobile application ID, browser type, browser language, type of operating system, and the date and time the End User visited a Publisher Site or Toolbar User used the Toolbar;

Behavior on a Publisher Site, such as how long the End User visited the Publisher Site, End User sharing behavior of content on a Publisher Site, and scrolling behavior of an End User on a Publisher Site;

The referring URL and the web search the End User used to locate and navigate to a Publisher Site;

Keywords entered into the AddThis Toolbar search functionality, and whether and when the Toolbar User downloads, installs, or uninstalls the AddThis Toolbar;

Information regarding how often an End User uses the AddThis Tools and how often a Toolbar User uses the AddThis Toolbar; and

Geo-location data derived from an End User’s and Toolbar User’s IP address.

TI IRELAND USE OF GOOGLE MAPS

We use the “Google Maps” component of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA, hereinafter “Google.”

Google sets a cookie in order to process the user configuration and data when the page with the integrated “Google Maps” component is displayed. As a general rule, this cookie is not deleted by

closing the browser, but rather expires after a certain time, as long as it is not previously manually deleted by you.

If you do not agree with this processing of your data, you may choose to deactivate the “Google Maps” service and thereby prevent the transfer of data to Google. To do this, you must deactivate the Java Script function in your browser. However, we would like to point out that in this case you will not be able to use “Google Maps” or at least only to a limited extent.

The use of “Google Maps” and the information obtained through “Google Maps” is according to Google’s Terms of Use

https://policies.google.com/termsas well as the additional Terms and Conditions for "Google Maps"

https://developers.google.com/maps/terms

USE OF FACEBOOK COMPONENTS

The TI Ireland Website employs components provided by facebook.com. Facebook is a service of Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA.

Each time the Website receives an access request equipped with a Facebook component, the component prompts your browser to download an image of this Facebook component. Through this process, Facebook is informed precisely which page of the TI Ireland Website is being visited.

When you access our site while logged into Facebook, Facebook uses information gathered by this component to identify the precise page you are viewing and associates this information to your personal account on Facebook. Whenever you click on the “Like“ button, for example, or enter a comment, this information is transmitted to your personal account on Facebook and stored there. In addition, Facebook is informed of your visit to the TI Ireland Website. This occurs regardless of whether you click on a component or not.

If you wish to prevent the transfer to and storage of data by Facebook about you and your interaction with the TI Ireland Website, you must first log out of Facebook before visiting the TI Ireland Website. The data protection policies of Facebook provide additional information, in particular about the collection and use of data by Facebook, your rights in this regard as well as the options available to you for protecting your privacy: https://www.facebook.com/about/privacy/

You can find an overview of Facebook plugins at https://developers.facebook.com/docs/plugins/

USE OF TWITTER RECOMMENDATION COMPONENTS

The TI Ireland Website employs components provided by Twitter. Twitter is a service of Twitter Inc., 795 Folsom St., Suite 600, San Francisco, CA 94107, USA.

Each time the TI Ireland Website receives an access request equipped with a Twitter component, the component prompts your browser to download an image of this component from Twitter. Through this process, Twitter is informed precisely which page of the TI Ireland Website is being visited. We have no control over the data that Twitter collects in the process, or over the extent of the data that Twitter collects. To the best of our knowledge, Twitter collects the URL of each website accessed as well as the IP address of the user, but does so solely for the purpose of displaying Twitter components. Additional information may be obtained from the Twitter data privacy policy, at: http://twitter.com/privacy.

You may change your data privacy settings in your account settings,
at http://twitter.com/account/settings

USE OF LINKEDIN RECOMMENDATION COMPONENTS

The TI Ireland Website employs components provided by the network LinkedIn. LinkedIn is a service of LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. Each time the TI Ireland Website receives an access request equipped with a LinkedIn component, the component prompts your browser to download an image of this component from LinkedIn. Through this process, LinkedIn is informed exactly which page of the TI Ireland Website is being accessed. By clicking the LinkedIn "recommend button" while logged into your LinkedIn account, you can link content from the TI Ireland Website to your LinkedIn profile. This allows LinkedIn to associate your visit to our site with your LinkedIn account.

We have no control over the data that LinkedIn collects thereby, nor over the extent of the data that LinkedIn collects. Nor do we have any knowledge of the content of data transferred to LinkedIn. Details on data collection by LinkedIn as well as your rights in this regard and your browser setting options may be obtained from the LinkedIn data privacy policy, which may be accessed at: http://www.linkedin.com/legal/privacy-policy

USE OF YOUTUBE COMPONENTS

On the TI Ireland Website we use components (videos) of YouTube, LLC 901 Cherry Ave., 94066 San Bruno, CA, USA, a company belonging to Google Inc., Amphitheatre Parkway, Mountain View, CA 94043, USA.

When you display a page that has an embedded video, a connection will be made to the YouTube server and the content will appear on the TI Ireland Website via a communication to your browser.

Further information about data protection by YouTube is provided by Google under the following link:

https://policies.google.com/privacy

USING PAYPAL AS A PAYMENT METHOD

If, while completing your donation, you decide to use PayPal as an online payment service, your contact details will be sent to PayPal during the order process. PayPal is a service from PayPal (Europe) S.à.rl & Cie. SCA, 22-24 Boulevard Royal, L-2449 Luxembourg. PayPal assumes the function of an online payment service and trustee, and offers buyer protection services.

The personal data transmitted to PayPal usually includes your first name, last name, address, telephone number, IP address, e-mail address, or other data required to process your donation.

This information needs to be transferred to process your order using your chosen payment method, mainly in order to confirm your identity and manage your payment and the customer relationship.

Please note the following however: PayPal may also pass on your personal data to subcontractors or other affiliates, to the extent necessary for fulfilling the contractual obligations arising from your order or for processing personal data in your order.

Depending on the payment type you pre-select in your PayPal account, which may include payment by invoice or direct debit, PayPal will transfer the personal data transferred to PayPal to credit agencies. The information transferred serves to identify you and to verify your creditworthiness with regard to the order you have placed. Please refer to the PayPal Privacy Policy for more information on the credit agencies PayPal transfers data to and which data is collected, processed, stored and passed on by PayPal: https://www.paypal.com/ie/webapps/mpp/ua/privacy-full

USING STRIPE AS A PAYMENT METHOD

For the purpose to proceed with payments we use Stripe. Stripe is a service from Stripe, Inc, 185 Berry Street, Suite 550, San Francisco, CA 94107, USA. Your data will be sent to a server operated by Stripe, Inc in the United States.

You can find more information about Stripe here:

https://stripe.com/privacy

Stripe also participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. For more information and to view the Privacy Shield policy, go here:

https://www.privacyshield.gov/participant?id=a2zt0000000L1HMAA0&status=Active

USE OF GOOGLE ADWORDS

For purposes of promotion, the TI Ireland Website also employs the Google ad tool "Google-Adwords". As part of this, the Website employs the analysis service "Conversion-Tracking" from Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA, hereinafter referred to as “Google“. If you access our site by way of a Google ad, a cookie is placed on your computer. Cookies are small text files that your internet browser downloads and stores to your computer. These so-called "conversion cookies" cease to be active after 30 days and are not used to identify you personally. If you visit certain pages of the Website while the cookie is still active, we and Google know that you, as user, have clicked on ads placed on Google and were redirected to our site. Google uses the information obtained through "conversion cookies" to compile statistics for the Website. These statistics tell us the total number of users who have clicked on our ad as well as which pages of our site were then accessed by each user. However, neither we nor other advertisers who use "Google-Adwords" receive any kind of information that can be used to personally identify users. You can prevent the installation of "conversion cookies" by making the appropriate change to your browser settings, for example by setting your browser so that the automatic placement of cookies is deactivated or by blocking cookies from the domain "googleadservices.com“.

You can obtain the relevant data privacy policy from Google at the following link:

https://policies.google.com/privacy

NEWSLETTER

The TI Ireland Website offers you the opportunity to subscribe to our newsletter. The newsletter provides you periodically with information about our services. You can view our Newsletter Privacy Policy for more information on how we safeguard your personal data.

APPENDIX 12: TEMPLATE RESPONSE FOR SUBJECT ACCESS REQUEST (cf Article 15 GDPR)

Dear XXX,

Thank you for your request for access to your personal data held by Transparency International Ireland. [Thank you for providing us with XXXX as proof of your identity. OR You need to provide us with a copy of your passport or driving licence as proof of identity before we can proceed with your request]

Your request, dated xx/xx/20xx, was received by us on xx/xx/20xx. We will respond to you before xx/xx/20xx [within one calendar month].

[If this is not possible, then write to the requestor as soon as possible to ask for an extension of time].

Please be advised that we hold the following categories of data for you:

Name; [Gender]; [Employer]; [File Reference Number]; [Trade Union Membership].

We processed your personal data in order to assess your call to the SpeakUp Helpline and to help identify what type of assistance we could provide to you in response to your enquiry. We also use statistics and general information from this database to pursue the legitimate interests of Transparency International Ireland to monitor patterns in corruption and wrongdoing, produce reports and formulate recommendations to policy-makers as appropriate.

We hold your data in hard copy and electronic form. The hard copy data is stored in our secure filing systems at our offices at 69 Middle Abbey Street, Dublin 1. This data is also held on a secure website hosted by the Transparency International Secretariat in Berlin. No-one except our Helpline staff and volunteers have access to the database. [**The data is transferred with appropriate safeguards as required by law and enforced by a data processing contract**]

We envisage storing your data for a period of six years. This is the period of legal limitation for pursuing a civil remedy in the Court for detriment suffered for having made a protected disclosure for the purposes of the Protected Disclosures Act 2014.

You have the right to request that any inaccurate that is held about you is corrected, or if we have incomplete information you may request that we update the information such that it is complete.

You also have the right to request that your personal data is not processed or is only processed in a certain way. You also have the right to request us to delete personal data that we hold about you.

If you have any queries or complaints in connection with our processing of your personal data, you can get in touch with us using the following contact details:

Post: Data Protection Officer, Transparency International Ireland, 69 Middle Abbey Street, Dublin 1

You also have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your personal data. Details of how to lodge a complaint can be found on the dataprotection.ie website, or you can call the Data Protection Commission on 1890 252 231.

APPENDIX 13: STAFF AND VOLUNTEER PRIVACY NOTICE

GDPR PRIVACY NOTICE

1. As your employer, TII needs to keep and process information about you for normal employment/internship purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of TII and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

2. We will process your personal data for the purposes of fulfilling your contract of employment / Volunteer Agreement.

3. Where we process special categories of personal data e.g. relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will process on the grounds that such processing is necessary for the required by law or the information is required to protect your health in an emergency.

4. Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees.

5. The sort of information we hold includes: your CV and references, your contract of employment and volunteer agreement and any amendments to it; proof of your academic credentials, such as Degree/Diploma Certificates, confirmation of your grades from your university or college, your membership details of professional bodies; information needed for payroll, benefits and expenses purposes (covering travel cards and details of travel); contact and emergency contact details; records of holiday, sickness and other absence; information needed for equal opportunities monitoring policy; and records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.

6. You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company.

7. Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay.

8. We will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to our accountant or pension schemes. Personal Data such as bank details which are collected for the purpose of payment of salary and benefits may be disclosed to the Revenue Commissioners, the Law Society of Ireland and other authorities for purposes of regulatory compliance.

9. In addition, we monitor computer and telephone use, as detailed in our Acceptable IT Use policy, as explained and signed by you at your induction.

10. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to our external payroll or pension provider.

11. Categories of employees who have access to personal data eg payroll staff, recruitment professionals.

12. We do not use automated decision making (including profiling).

13. Your personal data will be stored for the duration of your employment with us, plus a period of six years after the termination of employment. This will include your financial, tax and in come records as well as staff records (to include health information). References, pension and benefit records will be kept permanently.

14. If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.

Your rights

15. Under the General Data Protection Regulation (GDPR) you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

16. If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

17. You have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your personal data. Details of how to lodge a complaint can be found on the dataprotection.ie website, or you can call the Data Protection Commission on 1890 252 231.

18. Transparency International Ireland Limited is the controller and processor of data for the purposes of the DPA 18 and GDPR.

19. If you have any concerns as to how your data is processed you can contact: Donncha Ó Giobúin, Data Protection Offer at helpline@transparency.ie

APPENDIX 14: IAW MEMBERS PRIVACY NOTICE

Dear Integrity at Work Member,

I am writing to you about the General Data Protection Regulation (“GDPR”) which comes into effect on 25 May 2018. We think it necessary to send you details of how we hold and process the personal data of some of your staff members (“data”).

Your data is controlled and processed by Transparency International (TI) Ireland Limited and we are located at 69 Middle Abbey Street, Dublin 1.

If you have any queries or complaints or questions in relation to the processing of your data, you can contact TI Ireland's data protection officer. His name is Donncha Ó Giobúin and he can be contacted at: helpline@transparency.ie or on 01 554 3938.

In order to provide our services to you, we need to process certain data as follows: Names of your staff members; Email address of your staff members; Functions of your staff members; and correspondence on the functioning of the IAW Contract and services.

We are required to ensure that there is an appropriate basis for processing your data, and we are required to let you know what that basis is. Our legal basis for processing your data is for the performance of the IAW Membership contract which you entered into with us,and in order to contact you about conferences and other events. You must ensure you have provided the adequate notice or received the necessary consents to allow you to share any personal data with us relating to your employees. .

We will process your data in order to provide you with our services in accordance with the principles of the GDPR. We will only share your data with TI Ireland Associates. When we do share your data, we ensure that our Associates are compliant with the latest data protection legislation.

We hold your data in hard copy and electronic form. The electronic data is stored on a secure drive on our IT systems at our offices at 69 Middle Abbey Street, Dublin 1. No-one except Transparency International Ireland staff and volunteers have access to our IT systems. Any hard copy print-outs of your data will be stored in locked filing cabinets and we envisage storing the data for the period of our contractual relationship.

You have the right to request a copy of the personal data that we hold about you and to request that any inaccuracies in your data are corrected. If we have incomplete information you may request that we update the information such that it is complete.

You also have the right to request us to delete your data. You have the right to request that we longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes. You can also request that we provide you, or a third party, with a copy of your personal data in a structured, commonly-used, machine-readable format. There is no automated processing of the data that you provide to us.

You have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your data. Details of how to lodge a complaint can be found on the dataprotection.ie website, or you can call the Data Protection Commission on 1890 252 231.

A more detailed privacy policy can be found on www.transparency.ie

APPENDIX 15: TRAINING PARTICIPANTS PRIVACY NOTICE

Dear xxx,

Because you have agreed to participate in our training on xxx, on xxxx, it will be necessary for us to hold personal data about you in the form of your name, position, email address and any email correspondence about the training.

Your data will be controlled and processed by Transparency International Ireland Limited (Company No: 390950) and we are located at 69 Middle Abbey Street, Dublin 1.

If you have any queries or complaints in relation to the processing of your data, you can contact our data protection officer. His name is Donncha Ó Giobúin and he can be contacted at: helpline@transparency.ie or on 01 554 3938.

We will process this data in order to facilitate your attendance at the training. We will only share your data with TII Associates. When we do share your data, we ensure that our Associates are compliant with the latest data protection legislation.

We hold your data in hard copy and electronic form. The electronic data is stored a secure drive on our IT systems at our offices at 69 Middle Abbey Street, Dublin 1. No-one except our IAW staff and volunteers have access to our IT systems. Any hard copy print-outs of your data will be stored in locked filing cabinets and shredded after use.

We will store your personal data for the period of our contractual relationship with your employer.

You have the right to request a copy of the personal data that we hold about you and that any inaccuracies in your data are corrected. If we have incomplete information you may request that we update the information such that it is complete.

You also have the right to request us to delete your data. You have the right to request that we longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes. You can also request that we provide you, or a third party, with a copy of your personal data in a structured, commonly-used, machine-readable format. There is no automated processing of the data that you provide to us.

You have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your data. Details of how to lodge a complaint can be found on the dataprotection.ie website, or you can call the Data Protection Commission on 1890 252 231.

A more detailed privacy policy can be found on www.transparency.ie

APPENDIX 16: CONFERENCE PARTICIPANTS PRIVACY NOTICE

Dear xxx,

By signing up to our conference on xxx, on xxxx, we will hold personal data about you in the form of your name, position in your company, email address and any email correspondence about the conference.

Your data will be controlled and processed by Transparency International Ireland Limited (Company No: 390950) and we are located at 69 Middle Abbey Street, Dublin 1.

If you have any queries or complaints in relation to the processing of your data, you can contact our data protection officer. His name is Donncha Ó Giobúin and he can be contacted at: helpline@transparency.ie or on 01 554 3938.

We process the personal data we gather from you (i.e. name, email etc) in order to facilitate your attendance at the conference [and any other reason for which the data is used, and why its used in that way]. We will not share your data with any third party unless we are under a legal obligation to do so.

We hold your data in hard copy and electronic form. The electronic data is stored a secure drive on our IT systems at our offices at 69 Middle Abbey Street, Dublin 1. No-one except our IAW staff and volunteers have access to the database. Any hard copy print-outs of your data will be stored in locked filing cabinets and shredded after use.

We envisage storing the data for a period of five years after the conference.

You have the right to request a copy of the personal data that we hold about you and that any inaccuracies in your data are corrected. If we have incomplete information you may request that we update the information such that it is complete.

You also have the right to request us to delete your data. You have the right to request that we longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes. You can also request that we provide you, or a third party, with a copy of your personal data in a structured, commonly-used, machine-readable format. There is no automated processing of the data that you provide to us.

You have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your data. Details of how to lodge a complaint can be found on the dataprotection.ie website, or you can call the Data Protection Commission on 1890 252 231.

A more detailed privacy policy can be found on www.transparency.ie

APPENDIX 17: TII BOARD MEMBERS PRIVACY NOTICE

Dear Board Member,

We are writing to you about the General Data Protection Regulation ("GDPR") which comes into effect on 25 May 2018.

Your data is controlled and processed by Transparency International Ireland ("TI Ireland") (Company No: 552538) and we are located at 69 Middle Abbey Street, Dublin 1. Our legal basis for processing your data is compliance with the legal obligations under the Companies Act to which TI Ireland is subject.

The data we hold includes your name, address, email address, date of birth, and copies of identity documents and proof of address (such as passport/driving licence copies and copies of utility bills).

We also hold data on your Directorships of other companies, any relevant financial interests you are required by law to declare, any Board Minutes with a list of attendees, attendance sheets, and any email correspondence in relation to Board meetings and other business.

Your data is shared with the Companies Registration Office where necessary for compliance and our auditors for the purposes of our annual audited accounts. Your names are published on our website for governance purposes. Your data is not shared with anyone else.

If you have any queries or complaints in relation to the processing of your data, you can contact TI Ireland's Data Protection Officer, Donncha Ó Giobúin, Data Protection Offer at helpline@transparency.ie

We hold your data in hard copy and electronic form. The electronic data is stored on a secure drive on our IT systems at our offices at 69 Middle Abbey Street, Dublin 1. No-one except our Chief Executive, Office Coordinator, and Company Secretary have access to the data. Any hard copy print-outs of your data will be stored in locked filing cabinets and shredded after use.

We envisage storing the data for the period of your term of office as a Member of the Company or a Director of the Board after which period your data will be destroyed in line with our Data Retention and Destruction Policy.

You have the following rights under GDPR, in certain circumstances and subject to certain exemptions, in relation to your personal data:

1. Right to access the data – you have the right to request a copy of the personal data that we hold about you, together with other information about our processing of that personal data;
2. Right to rectification – you have the right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information you may request that we update the information such that it is complete.
3. Right to erasure – you have the right to request us to delete personal data that we hold about you.
4. Right to restriction of processing or to object to processing – you have the right to request that we no longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes.

5. Right to data portability – you have the right to request us to provide you, or a third party, with a copy of your personal data in a structured, commonly-used, machine-readable format.

In order to exercise any of the rights set out above, please contact us at the contact details above.

You have the right to lodge a complaint with the Data Protection Commission if you are unhappy with our processing of your data. Details of how to lodge a complaint can be found on the dataprotection.ie website, or you can call the Data Protection Commission on 1890 252 231.

APPENDIX 18: NON-DISCLOSURE AGREEMENT

I, _____, acknowledge that the information received or generated, directly or indirectly, while working as a Volunteer/Associate/Staff Member or Board Member for Transparency International (TI) Ireland is confidential and that the nature of the business of TI Ireland is such that the following conditions are reasonable, and therefore:

I warrant, covenant and agree as follows:

I agree not to disclose, directly or indirectly, any information with respect to any business conducted by TI Ireland.

Without restricting the generality of the foregoing, it is agreed that:

- I will not disclose financial information, business plans, strategies for development or growth, or any other proprietary information not known generally to the public or in the public domain relating in any way to the business of TI Ireland, or any other information regarding the management or method of operation of TI Ireland, and
- I will not disclose information of personal details and personal data of clients, members, volunteers or other people which is stored by the organisation
- I will not copy or reproduce, in any form, information provided to me by TI Ireland for the purpose of distribution or use outside the scope of the attached contract, and that all documentation provided to me will be returned to TI Ireland unless otherwise approved, in writing, by the Chief Executive of TI Ireland.

This obligation of confidence shall continue after the conclusion of the contract of volunteer engagement.

I acknowledge that the aforesaid restrictions are necessary and fundamental to the business of TI Ireland, and are reasonable given the nature of the business carried on by TI Ireland.

I agree that this agreement shall be governed by and construed in accordance with the laws of the Republic of Ireland. I agree that each provision of this agreement is separate and distinct, and is severable from all other separate and distinct provisions.

If any of the activities, periods of time, or other matters contained in this agreement are considered by a court of competent jurisdiction as being unreasonable, the court shall have the authority to limit such matters as the court deems proper in the circumstances and if any provision is void or unenforceable in all or in part, it shall not affect the enforceability of the balance of this agreement.

TI Ireland shall be entitled and has the right to obtain an injunction to ensure compliance with this agreement.

I enter into this agreement totally voluntarily, with full knowledge of its meaning, and without duress.

Signed _____,

Dated _____,

Signed on behalf of Transparency International Ireland

_____,

Dated _____,

JOB APPLICANT PRIVACY NOTICE

As part of any recruitment process, Transparency International Ireland ('TI Ireland') collects and processes personal data relating to job applicants. TI Ireland is committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

What information do we collect?

TI Ireland collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the Ireland.

TI Ireland may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

We may also collect personal data about you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

Data will be stored securely in a range of different places, including on your application record, management systems and on other IT systems (including email).

Why does TI Ireland process personal data?

TI Ireland has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process in order to recruit new staff. Processing data from job applicants allows us to recruit new employees , assess and confirm a candidate's suitability for a specific role and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims. We may also send you emails about your application through our email service provider.

TI Ireland may need to process your data to enter into a contract with you. In some cases, we need to process data to ensure that we are complying with its legal obligations. For example, it is mandatory to check a successful applicant's eligibility to work in Ireland before employment starts.

TI Ireland may process special categories of data, such as whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. We process such information to carry out our obligations and exercise specific rights in relation to employment. If your application is unsuccessful, TI Ireland may keep your personal data on file in case there are future employment opportunities for which you may be suited. We will ask for your consent before keeping your data for this purpose and you are free to withdraw your consent at any time.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the recruitment team, interviewers involved in the recruitment process, relevant managers, and IT consultants if access to the data is necessary for the performance of their roles. Members of the TI Board may from time-to-time be involved in the recruitment process.

Where an applicant is shortlisted for a second-round interview, they may be required to undergo a psychometric evaluation. Your personal data will be shared with an external consultant to setup the examination. You will be asked for your consent before any personal data is shared.

Should your application for employment be successful and we make you an offer of employment, we will make enquiries with your former employers to obtain references for you, employment background check providers to obtain necessary background checks.

How does TI Ireland protect data?

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. For more details, please see our data protection policy on the following website:
https://www.transparency.ie/sites/default/files/18.05.25_tii_data_protection_policy.pdf

For how long does TI Ireland keep data?

If your application for employment is unsuccessful, the organisation will hold your data on file for one year after the end of the relevant recruitment process. At the end of that period, your data is deleted or destroyed.

You will be asked when you submit your CV whether you give us consent to hold your data. If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your Human Resources file (electronic and paper based) and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request in a structured, commonly used, machine-readable format;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where TI Ireland is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Donncha Ó Giobúin at admin@transparency.ie. If you believe that the organisation has not complied with your data protection rights, you can complain to the Data Protection Commission.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to TI Ireland during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.