TRANSPARENCY
LEGAL ADVICE CENTRE

DATA PROTECTION POLICY

1. Introduction

The purpose of this document ("Policy") is to provide a concise policy statement regarding the data protection obligations of the Transparency Legal Advice Centre ("TLAC"), including under domestic law, the Data Protection Act 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) ("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, TLAC 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 special categories of personal data, undertaken by TLAC in the course of its activities. Transparency International Ireland Limited ("TII") provides all resources to TLAC and therefore is a data processor on TLAC's behalf.

3. Scope

The Policy applies equally to all personal data, whether in manual or automated form. All personal data, including sensitive 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 TLAC clients, Privacy Notice for Website (attached as Appendices 1-11 to the Policy).

4. Definition

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 automaticallyin response to instructions given for that purpose or

	(b) is recorded with the intention that it should be processed by meansof 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	TLAC (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 TLAC (excluding employees and volunteers of TLAC, processing personal data on behalf of TLAC Data in the course of his/her employment).
Data Protection Officer	A person appointed by TLAC to (a) inform and advise TLAC 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. TLAC as Data Controller and Data Processor

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

- TLAC Clients once referred from the TII Speak Up Helpline
- Job and volunteer/internship applicants
- Employees
- Volunteers
- Third party service providers engaged by TLAC
- Board members and company members
- Supporters/donors/funders

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, TLAC 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 TLAC'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 Managing Solicitor is immediately informed, in order that appropriate corrective action is taken.

6. Records of Processing Activities (need to confirm whether this is necessary)

TLAC 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 controller, 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, TLAC may engage third parties to process Personal Data on its behalf ("Data Processors"). In this regard, TLAC 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 TLAC, 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. TLAC has identified the following organisations who process data on its behalf: TII, Firm Central and Angela Maguire, the TLAC accountant.

TII processes data on behalf of TLAC pursuant to a data processing agreement.

Regular audit trail monitoring will be undertaken by the Managing Solicitor of TII 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 be obliged to cooperate with the Office of the Data Protection Commissioner 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 TLAC for a copy of their personal data (a "Subject Access Request") will be referred, as soon as possible, to the Managing Solicitor of TII, 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. TLAC 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 TLAC 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, TLAC 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, TLAC will provide the Data Subject with the information stipulated in Article 15(1) GDPR, where applicable.

A Subject Access Request may be refused by TLAC on the basis that it is manifestly unfounded or excessive, in particular because of its repetitive character. TLAC will bear the burden of demonstrating the manifestly unfounded or excessive nature of any such request. TLAC 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 TLAC 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 (the right to be informed and right of access);
- A right to request that any incomplete information be updated such that it is complete (the right to rectification);
- A right to request the controller to delete personal data held (the right to erasure);
- 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 (the right to restrict processing and the right to object);
- A right to request a copy of personal data in a structured, commonly used machine readable format (the right to data portability).

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, TLAC 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 TLAC, TLAC 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 TLAC, being the Data Controller;

(b) the contact details of the 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 TLAC 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 TLAC 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 TLAC 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 Article22(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.

TLAC 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.

TLAC meets these obligations in the following ways:

- A privacy notice is read and signed by TLAC Clients on initial appointment. This Privacy Notice is also sent in the letter of engagement (see Appendix 10).
- 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. This 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.

9.2 Lawful Basis for Processing:

TLAC processes employee or volunteer personal data on the following grounds:

- Such processing is necessary for the performance of a contract between TLAC and its staff (Art 6(1)(b) GDPR).
- In the case of volunteers, such processing is necessary for the legitimate interest of TLAC (Art 6(1)(f) GDPR) to check the identity and competence of volunteers to ensure the quality and consistency in the services provided by TLAC.

TLAC processes personal data of TLAC Clients on the following grounds:

- The processing of personal data is necessary for the performance of a contract as set out in between TLAC and the Client, i.e. the letter of engagement ii) the legitimate interests of the data controller, that being the provision of legal advice iii) consent, as obtained in initial consultation with the client.(Art 6(1)(b) GDPR)

- The processing is necessary for the legitimate interests pursued by TLAC (Art 6(1)(f) GDPR), that being the provision of legal advice to individuals facing an ethical dilemma at work.
- To the extent that TLAC processes special categories of data, the processing of such data 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).
- TLAC processes personal data of Board Members is necessary for compliance with TLAC's legal obligations under the Companies Act 2014 (Art 6(1)(c)).
- TLAC 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 TLAC 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 (as per the TLAC Privacy Notice to be signed on initial consultation).

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

TLAC will continue to process data in pseudonymised form for statistical purposes. TLAC will not further process Personal Data in a manner incompatible with the specified, explicit and legitimate purposes for which it was collected.

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

TLAC will employ high standards of security in order to protect the Personal Data under its care. TLAC's Password Policy (Appendix 6), 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.

Volunteer Recruitment Data

All Volunteer Recruitment data is stored on secure IT systems. Access is restricted to TLAC's Managing Solicitor. CVs are kept on file for a year. No hard copies of the CVs are kept, if CVs are printed for interview purposes, they are shredded after use. CV's are not shared within other personnel without the consent of the data subject. On receipt of the application for a position, the applicant volunteer will be emailed with a Privacy Notice and informed of the lawful basis for processing of their personal data.

Staff Recruitment Data

All recruitment data related to staff is kept on a secure drive on our IT systems. Access is restricted to Managing Solicitor within the organisation. CVs are kept on file for a year. No hard copies of the CVs are kept, if CVs are printed for interview purposes, they are shredded after use. CV's are not shared

within other personnel without the consent of the data subject. On receipt of the application for a position, the applicant volunteer will be emailed with a Privacy Notice and informed of the lawful basis for processing of their personal data.

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. This data is processed in accordance with TLAC's legitimate interests. 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 Managing Solicitor. 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 data) is stored in hard copy in a locked cabinet. This data is processed in accordance with TLAC's legitimate interests, and for the performance of the contract of employment with the member of staff. This information is kept on file for ten 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 the Managing Solicitor. 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 in hard copy in a locked cabinet. This data is processed in accordance with TLAC's legitimate interest. This information is kept on file for three years after the departure of the Board Member. Access is restricted to the Managing Solicitor. If this material is printed in hard copy it will be shredded after use.

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 Managing Solicitor. The hardcopy minutes are saved in a secure filing system. 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

Volunteer Recruitment

This will be kept accurate and up-to-date by the Managing Solicitor. The Managing Solicitor will review and amend the data when notified of a change, will document the legitimate bases 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 Managing Solicitor. The Managing Solicitor will review and amend the data when notified of a change, will document the legitimate bases 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 Managing Solicitor. The Managing Solicitor will review and amend the data when notified of a change, will document the legitimate bases 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 Managing Solicitor. The Managing Solicitor will review and amend the data when notified of a change, will document the legitimate bases 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 Managing Solicitor / Company Secretary. The Managing Solicitor/Company Secretary will review and amend the data when notified of a change, will document the legitimate bases 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 Managing Solicitor / Company Secretary. The Managing Solicitor / Company Secretary will review and amend the data when notified of a change, the consent document and the legitimate bases for the processing of data, diarise data retention/destruction periods and deal with any subject access requests.

TLAC will review and update staff contact details and details of next-of-kin every two years.

9.6 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.

TLAC 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.

TLAC 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, TLAC 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

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

The Managing Solicitor 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 TLAC.

The Managing Solicitor 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 TLAC'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 TLAC ("TLAC"), you will need to submit a written request, to the Managing Solicitor, Transparency Legal Advice Centre, Floor 3, 69 Middle Abbey Street, Dublin 1.

In order that TLAC 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 TLAC processes a large quantity of information concerning you, please specify in your request the information you require.

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

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

In responding to a Subject Access Request, TLAC 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~~er~~;
- 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.

Where a request is manifestly unfounded or excessive, TLAC 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, under section 60 of the Data Protection Act 2018, personal data can be withheld under certain circumstances, as set out in the amended Section 4.

Updated: 14 January 2020

APPENDIX 2: DATA RETENTION AND DESTRUCTION POLICY

The purpose of this Data Retention and Destruction Policy is to ensure that TLAC ("TLAC") 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 TLAC 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 Managing Solicitor

The Managing Solicitor 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 TLAC; (b) monitor the compliance of TLAC's employees (and volunteers etc?) with this Policy; and (c) take such other action as may be authorised by TLAC's Board of Directors. c. Distribution of policy to staff members and volunteers

The Managing Solicitor 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 Managing Solicitor, unless the Managing Solicitor 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 TLAC reasonably anticipates or becomes aware of an audit or the commencement of any litigation against or concerning TLAC, such employee shall inform the Managing Solicitor and any further destruction of personal data shall be suspended until such time as the Managing Solicitor determines otherwise. The Managing Solicitor 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 Managing Solicitor. 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. 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**
TLAC	Legal File	Six years, legal limitation expiry	Managing Solicitor
	Electronic Entry on Firm Central	Six years, legal limitation expiry	Managing Solicitor
Volunteer Recruitment	CV/email/correspondence	1 year after recruitment concluded (limitation for Equality Act claim)	Managing Solicitor

Staff Recruitment	CV/email/correspondence	1 year after recruitment concluded (limitation for Equality Act claim)	Managing Solicitor
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	Managing Solicitor
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,	Managing Solicitor
		pension and benefit records – these should be kept permanently	
Board Member Data	Identity/Qualifications/Bank details	3 years after the end of the Directorship	Managing Solicitor/Company Secretary
Board Data	Board of Directors' records including minutes of meetings	Permanently	Managing Solicitor/Company Secretary
	Bank information/email addresses on funders/donors/other supporters	Permanently	Managing Solicitor/Company Secretary

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

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

Updated: 14 January 2020

Updated: 14 January 2020

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 the Transparency Legal Advice Centre ("TLAC") 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 Commissioner in 2011.

2. Rationale

The response to any personal data breach can have a serious impact on TLAC's reputation and the extent to which the public perceives TLAC 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 TLAC. The policy applies all personal data, whether in manual or automated form. All Personal Data will be treated with equal care by TLAC.

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 TLAC's Managing Solicitor.

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

6. When will the Data Protection Commission be informed?

In cases of a personal data breach, the Managing Solicitor 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 Managing Solicitor 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 TLAC 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.

TLAC 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 TLAC'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, TLAC 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 TLAC 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) TLAC 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) TLAC 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

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

APPENDIX 5: DATA SHARING/PROCESSING AGREEMENT

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

TLAC ("TLAC") 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 party organisation/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 2019 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").

[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.

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

[Third Party Organisation/Agency] agrees to assist TII in complying with TII's obligations toward data subjects, including taking reasonable steps to assist TII in notifying personal data breaches to the Data Protection Commission, communicating such breaches to data subjects, and carrying out assessments of the impact of any personal data breach.

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.

[Consider inserting clauses relating to designation of a DPO; transfers of personal data to third countries or international organisations where appropriate; mechanisms for resolving disputes regarding respective liabilities for claims].

Parties to this agreement:

_____ Date: _____

Name

[Role], Transparency International Ireland

_____ Date: _____

Name

[Role], [Third Party Organisation/Agency]

Updated: 14 January 2020

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 TLAC files.

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

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 TLAC facility, has access to TLAC network, or stores any non-public TLAC 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 clustersystems or public terminals.
- All system-level passwords must be changed on at least a bi-yearly basis by TLAC's third-party IT Company.
- All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at leastevery six months.
- Passwords must not be inserted into email messages or other forms of electroniccommunication.
- 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 TLAC 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 TLAC accounts from other non TLAC access.
- Always use different passwords for various TLAC access needs whenever possible.
- Do not share TLAC 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.
- 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 Managing Solicitor.
- 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.

Updated: 14 January 2020

Password cracking or guessing may be performed on a periodic or random basis by TLAC's thirdparty 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 userlevels is to be encrypted.

Updated: 14 January 2020

APPENDIX 7: REMOTE ACCESS POLICY

1. Overview

Consistent standards for network access are critical to Transparency Legal Advice Centre ("TLAC")'s information security. Any staff member accessing TLAC'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 the TLAC network from a desktop computer, laptop or any device located outside TLAC's network.

This policy is mandatory for all staff members of TLAC 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 companyprovided 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 TLAC to provide goods and services (for example: technical support, consultancy etc) and who require access to TLAC 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 Managing Solicitor.

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 TLAC 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 TLAC 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. TLAC 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 TLAC'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 TLAC network(s) or information systems that originates from a computer or device located outside of TLAC'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 Legal Advice Centre ("TLAC")'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. **WD TLAC**

   Organisational files and casework files. This is accessible by all staff members and volunteers.

2. Speak Up database

Accessible to helpline staff and volunteer

Updated: 14 January 2020

APPENDIX 10: PRIVACY NOTICE FOR TLAC CLIENTS

Article 12 and 13 of GDPR

As our client, we owe you a duty of confidentiality, which we will strictly observe. No information which you give to us or any legal advice we give to you will be shared with any third party without your consent except in accordance with this Privacy Policy, unless required to do so by law. TLAC is required to report instances of potential criminal offences committed against minors or vulnerable adults to Tusla, An Garda Síochána and other relevant authorities. TLAC 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.

In signing the declaration at the bottom of this letter, you are providing us with consent to hold information about you, including sensitive information such as medical details or membership of a Trade Union. You are free to withdraw your consent at any time and can do so by contacting me by telephone or email. 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. You acknowledge that TLAC will process your personal data in accordance with this Privacy Notice. TLAC relies on its legitimate interest to process your personal data, i.e. the provision of legal advice to individuals facing an ethical dilemma at work. To the extent that TLAC processes your sensitive personal data, it will do so in pursuit of a substantial public interest, namely the prevention of corruption and abuses of power in the workplace.

We will treat your case confidentially and we will use your personal information solely to provide our agreed services to you. We will not reveal to any third party any details that could identify you, unless you have given us permission to do so or we are legally required to make such a disclosure.

From time to time, we may pass information to other organisations in respect of the outcomes of our cases. However, we will only do this in a way that will not identify you personally. If you have any concerns about this, please discuss these with us.

Once this matter is concluded, we will keep a copy of your paperwork for at least 6 years. Following this period, we will keep a copy of your personal data in a pseudonymised format for statistical purposes. The only person with access to the data will be the Data Protection Officer. You are entitled to request a copy of your personal data.

We are the data controller for the purposes of data protection legislation. TII is a processor of your data and provides TLAC with all funding and resources necessary for the operation of TLAC. If you have any queries regarding the processing of your data, please direct them to TII. TII's address is 69 Middle Abbey Street, Dublin 1.

TLAC may transfer your personal data to TII for a number of data processing purposes, including statistical reporting on corruption, the production of TII's annual report, and for

the purposes of engaging with employers that are a member of the Integrity at Work programme.

You have a right to request from us access to and rectification or erasure of personal data. You have the right to request that we no longer process erasure of your personal data for particular where it is no longer necessary for the purposes or for which we are processing it. You have the right to object to our processing of your personal data for particular, however we may continue to process such data upon demonstrating a compelling legitimate interest. 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 e.g. on a disk.

If you wish to access a copy of the personal information we hold about you, please contact me on the following email address: joloan@transparencylegal.ie or Donncha Ó Giobúin at admin@transparency.ie.

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 on how to lodge a complaint can be found on the following website: www.dataprotection.ie or you can call the Data Protection Commission on 1890 252 231.

I, _____, declare that I have read and understood the above Privacy Notice, and freely give my consent to acknowledge that the Transparency Legal Advice Centre, to will process my personal data, including my sensitive personal data, pursuant to the lawful bases set out above for the purposes of providing you with legal advice on the application of the Protected Disclosures Act 2014 to your my circumstances

Updated: 14 January 2020

APPENDIX 11: PRIVACY NOTICE FOR WEBSITE

We Respect Your Privacy

Transparency Legal Advice Centre ("TLAC") is committed to ensuring the privacy of all our users. We collect and retain only such personal information as you choose to provide us. All such information is stored securely and will not be made public, sold, rented or likewise distributed.

TLAC's website is hosted as part of the http://www.speakup.ie ("TII Website"), including all information and materials contained on it is managed by TLAC and Transparency International Ireland, Floor 2, 69 Middle Abbey Street, Dublin 1.

This Privacy Policy governs all pages on www.speakup.ie. It does not apply to pages hosted by other organisations, including the websites of related organisations or third party sites. The TII Website may be linked to the websites of such other parties but those other sites may have their own privacy policies which apply to them.

By using the TII Website your consent is in accordance with the terms of this Privacy Policy. TII may change the terms of this Privacy Policy from time to time and if such changes are made, we may place notices on the TII Website so that you can be aware of them. Your continued use of the TII Website will be on the terms of this Privacy Policy as amended. Use of anonymous data collected by TII

Our web servers collect anonymous data about visits to the TII Website. This information is stored in log files and used to create aggregate statistics about when the TII Website is accessed, which pages refer visitors to us, the type of web browsers visitors use, which pages are viewed, etc. These statistics help us understand how the TII Website is used and provide us with valuable information for improving it for you in the future. This data cannot be used to identify you personally.

Use of personal data collected by TII

We do not collect any information from the TII Website that can be used to identify you unless you choose to provide it. For example, if you donate to TII, you can provide additional personal contact or payment information.

Personal information you submit to TII is kept confidential, is stored securely, and is retained only for as long as it is required for the purpose for which it was given. Personal information you provide will not be sold or rented or made public. Personal information is never shared with third parties unless we have your permission or are required to disclose the information by law, with the exception of the following circumstances:

Payment processing and fraud: If you make an online purchase or donation, your card details will be disclosed to a bank so that payment can be processed. In the case of a suspected fraudulent transaction, these details may be disclosed to the appropriate authorities for the sole purpose of investigation.

Updated: 14 January 2020

Hosting and processing: the TII Website is hosted by a third party service provider. We may also use third parties to process donations to TII. These third party services providers will process your personal information only on TII's behalf and are bound by strict confidentiality conditions.

Processing of your information by TII and its service providers is regulated by Irish data privacy law and protected by appropriate security measures.

Use of cookies

A cookie is a text-only piece of information that a website transfers to your computer's hard disk so that the website can remember your computer.

We may use cookies on the TII Website to do things such as control the behaviour of automatic popup surveys so they don't pop up every time you visit.

Our site statistical analytics software may use a cookie to track visitor navigation on our site, so we can tell how many times pages are visited, what countries visitors come from, whether they are first time visitors or regular visitors, and so on. You cannot be personally identified from this information.

To prevent the download of cookies, or otherwise control how cookies are used on your computer, please read the help information supplied with your Internet browser software, or go to: http://www.allaboutcookies.org/

Access to your personal information

If you have provided TII with personal information, under data protection laws you have the right of access to it in order to verify or correct it. In some circumstances you can object to our use of your information. If you wish to exercise any of these rights or have any questions about this policy, please contact:

Transparency International Ireland Limited

Floor 3

69 Middle Abbey Street

Dublin 1

Ireland

Or email helpline@transparency.ie

Updated: 14 January 2020

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 Legal Advice Centre. [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 provide you with legal advice on the application of the Protected Disclosures Act 2014 to your circumstances.

We hold your data in hard copy and electronic form. The hard copy data is stored in a locked filing cabinet and access is restricted to TLAC staff and volunteers. Access to the online database is on the basis of a password and is restricted to TLAC staff and volunteers.

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: Managing Solicitor, Transparency Legal Advice Centre, 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 23

APPENDIX 13: STAFF AND VOLUNTEER PRIVACY NOTICE

GDPR PRIVACY NOTICE

As your employer, TLAC needs to keep and process information about you for normal employment/internship purposes. TLAC is located at located at 69 Middle Abbey Street, Dublin 1 and can be contacted on 01 554 3957. 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/obligations that TLAC might be subject to , pursue the legitimate interests of TLAC 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.

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

Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not do so where required by law or the information is where required to protect your health in an emergency. Where we are processing data based on your consent, you have the right to withdraw that consent at any time. You can withdraw your consent by speaking to your line manager or the TLAC Managing Solicitor. Please note that if you withdraw your consent we may not be able to continue our employment/volunteer relationship with you.

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.

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.

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.

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.

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.

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.

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.

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

Your personal data will be stored only for the duration of your employment with us, and for 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.

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

Under the General Data Protection Regulation (GDPR) you have a number of rights with regard to your personal data. You have a right to request from us access to and rectification or personal data. You have the right to request erasure of your personal data, where it is no longer necessary for the purposes for which we are processing it. You have the right to restrict processing, object to our processing as well as in certain circumstances the right to data portability. of your personal data, however we may continue to process such data upon demonstrating a compelling legitimate interest. 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 e.g. on a disk

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.

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.

Transparency International Ireland Limited is the controller and processor of data for the purposes of Irish Data Protection legislation and GDPR.

If you have any concerns as to how your data is processed you can contact TLAC's Managing Solicitor or the Data Protection Officer Donncha Ó Giobúin at admin@transparency.ie or on 01 554 395

Updated: 14 January 2020

APPENDIX 14: BOARD & COMPANY MEMBER PRIVACY NOTICE

Dear Board and Company Member,

We are 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 your personal data.

Your data is controlled and processed by Transparency Legal Advice Centre ("TLAC") (Company No: 552538) and we are located at 69 Middle Abbey Street, Dublin 1. TII is a processor of your data and provides TLAC with all funding and resources necessary for the operation of TLAC. If you have any queries regarding the processing of your data, please direct them to TII. TII's address is 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 TLAC is subject. We otherwise hold your data for our legitimate interest, namely the operation of our organisation.

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 TLAC's Data Protection Officer, Judy O'Loan, at joloan@transparencylegal.ie or Donncha Ó Giobúin at admin@transparency.ie on 01 554 3957.

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 Managing Solicitor 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 your data is retained for the duration of your term of office as a Member of the Company or a Director of the Board after which period your data will be securely shredded.

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

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;

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.

Right to erasure – you have the right to request us to delete personal data that we hold about you.

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.

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.

Yours sincerely

Updated: 28 May 2019

APPENDIX 15: 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 the Transparency Legal Advice Centre ("TLAC") 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 TLAC, and are reasonable given the nature of the business carried on by TLAC.

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.

TLAC 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 _____ Date:

Signed on behalf of TLAC _____ Date:

Appendix 16: JOB APPLICANT PRIVACY NOTICE

As part of any recruitment process, TLAC collects and processes personal data relating to job applicants. TLAC 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?

TLAC 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.

TLAC 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 TLAC process personal data?

TLAC 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.

TLAC 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.

TLAC 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, TLAC 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 TLAC 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 such processing of your personal data is shared will be on the basis of our legitimate interest.

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 in a structured, commonly used, machine-readable format on request;
- 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 TLAC 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.

Appendix 17: DONATIONS

Online Donations

If you make a donation to the Transparency Legal Advice Centre (TLAC) or become a member of Friends of Transparency, you will be asked to provide the following personal data when making an online donation:

- Your first and last name
- Your email address
- Your Phone number

TLAC uses third party payment service providers to facilitate processing of your donation. TLAC has data processing agreements in place with each third party to ensure the that appropriate technical and organisational safeguards are used to protect your personal data.

You will be asked to provide your credit/debit card number, or your Paypal login details when making an online donation. TLAC does not receive these details. They are transmitted directly to our payment providers Stripe, Donorbox, and Paypal.

Using Donorbox as a payment method

While completing a donation online, you will be asked to provide personal data to Donorbox. Donorbox is a service provided by Rebel Idealist LLC, located at 5 3rd St, Suite 900, San Francisco, CA 94103.

You can learn more about Donorbox's Privacy Policy here: https://donorbox.org/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