The Thalidomide Trust

Suppliers Privacy Notice

1. Introduction

We are committed to protecting your personal data (any data that can identify you as an individual).

This privacy notice sets out our obligations and explains how we process (collect, store, use and share) your personal data, and how we look after it. It also tells you about your rights and how to contact us, and is based upon our overall Data Protection Policy.

This privacy notice is a part of our commitment to complying with our obligations under the UK General Data Protection Regulations (UK GDPR). It applies to current, prospective and former suppliers of goods and services to the Trust. The term 'suppliers' in this context includes representatives or contacts of organisations, freelance and independent contractors or consultants, and non-beneficiary volunteers[1]). This notice does not form a part of any other contract to provide goods and services and may be amended from time to time. We welcome your feedback to help make it even clearer. We will only process your personal data in the ways described in this privacy notice. This document may be amended from time to time and the latest version can always be found by contacting your DPO below.

At the Trust, protecting your personal data is very important to us, and we will only use your data as the law allows us to and which adheres to the UK GDPR principles of:

- Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Purpose limitation – data must be collected only for specified, explicit and legitimate purposes.
- Data minimisation – data must be adequate, relevant and limited to what is necessary.
- Accuracy – data must be accurate and, where necessary, kept up to date. Inaccurate data must be erased.
- Storage limitation – data must only be stored for as long as is necessary.
- Integrity and confidentiality – data must be processed in a secure manner.
- Accountability – the data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

[1] Beneficiary volunteers should refer to the Beneficiary Privacy Notice that can be found at: https://www.thalidomidetrust.org/wp-content/uploads/2023/03/Beneficiary-Privacy-Notice-March-2023.pdf

2. Who are we and how can you contact us?

The Thalidomide Trust Company (the Trust) – registered charity number 266220 – of 1 Eaton Court Road, Colmworth Business Park, Eaton Socon, St Neots, Cambridgeshire, PE19 8ER and **http://www.thalidomidetrust.org** – is the "data controller" for the purposes of data protection legislation. A data controller determines the purposes and means of processing personal data.

The Finance Director is the Data Protection Officer (DPO) for the Trust. The purpose of this role it is to ensure that data protection is an important part of the organisation's culture and working practices. If you have any questions about the use of your personal data, you should contact the Finance Director in the first instance:

By email to **hello@thalidomidetrust.org**

By telephone on 01480 474074

By writing to the Finance Director at the address above.

3. Definitions

Some words and phrases that we use in this privacy notice are defined here:

- "consent" means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them
- "data controller" means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this privacy notice, the Trust is the data controller of all personal data relating to workforce data subjects
- "data processor" means a person or organisation which processes personal data on behalf of a data controller
- "Data Protection Legislation" means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation
- "data subject" means a living, identified, or identifiable individual about whom the Trust holds personal data (in this context, workforce data subjects)
- "EEA" means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway

- "personal data" means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 data subject
- "personal data breach" means 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
- "processing" means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person, and
- "special category personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

4. What Personal Data do we Collect?

The personal information we may hold on you as a supplier to the Trust might include:

- personal details (such as name and job title)
- contact details (such as personal address, phone number and email address)
- financial information (such as bank account details)
- qualifications and professional experience
- references and results of DBS checks, including details of unspent convictions.
- details in references we have received about you and that we give to others
- security information (such as CCTV footage when visiting the Trust offices).

We will never hold any special categories of personal data (such as information about your health, your race or ethnicity, religious beliefs, sexual orientation and political opinions, or trade union membership).

We collect personal information about our suppliers from you directly as part of the process of becoming a supplier; from third parties as part of the process of becoming a supplier; and information obtained about you in the course of our working relationship. Personal data is collected in many ways: through communications with you either face to face or in writing, email or on the telephone; through monitoring of our websites, CCTV and access control systems, communications systems, email and internet facilities.

We may sometimes collect additional information from third parties including trade references, credit reference agencies, the DBS and other background check agencies.

We aim to ensure that our data collection and processing is always proportionate. We will notify you of any material changes to information we collect.

The provision of all this personal data is necessary in order that the Trust can enter into a contract with you to provide goods or services for the organisation and our beneficiaries. If you do not agree to provide the details requested, we may be unable to comply with the terms of any contract or our legal obligations to you, which may in turn result in us no longer being able to use you as a supplier.

5. How do we use your Personal Data?

We process the personal data of our suppliers for the following purposes:

- The process of applying for and becoming a supplier (such as making a decision about procuring goods or services)
- Managing our contract with you
- Reviewing the services or goods you supply to us or our beneficiaries
- Making payments to you for goods and/or services
- Dealing with complaints (such as gathering evidence in relation to any complaints made by or about you)
- Dealing with any legal disputes involving you)
- Complying with health and safety obligations
- Complying with other legal obligations, such as to prevent fraud.

For more information, please see section 7 which explains our lawful basis for processing your personal data.

You should be aware that certain roles within the organisation, which require direct contact with our beneficiaries, may require either a basic, standard, enhanced or enhanced with

barred list information DBS check to be carried out. We will only require a DBS check to be made where the role is eligible, and the check shall be at the appropriate level only and no higher. We will assess the relevance of any cautions and convictions detailed in the DBS check to the role for which the applicant has applied. A copy of your DBS certificate will be kept on your HR file and access to this will be limited to the Executive Director, your line manager, Office Manager and yourself.

An automated decision is one that is made with no human involvement, for example, where an organisation uses a computer system to score and select suppliers through a tender process. We do not undertake automated decision-making.

6. Cookies

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

Our website uses cookies to track user activity on the website (for example so we know how many unique visitors we have to the website and which pages are most visited) and to enable various types of functionality. They are never used for advertising purposes.

Details of our cookie policy are provided on the Trust website and all visitors are asked to accept/reject our use of cookies as soon as they access the website.

7. What is our Lawful Basis for Processing your Personal Data?

We will only use your personal data when the law allows us to. The UK GDPR sets out six legal bases for processing personal data. The most common legal bases for processing your personal data are:

- Where we need to fulfil the **contract** we have entered into with you.
- Where we need to comply with a **legal obligation**.
- Where it is necessary for our **legitimate interests** (or those of a third party) and your interests and fundamental rights do not override those interests.

In some cases there may be several grounds which justify our use of your personal data.

We will not, generally, rely on consent as a lawful basis for processing personal data but in certain circumstances it may be deemed appropriate. Where you provide consent to the processing of your data, you will be asked at the time the data is processed and you should be aware that you will be able to withdraw your consent at any time.

8. How do we Keep your Personal Data Secure?

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if the third party agrees to comply with those procedures and policies, or if it puts in place adequate measures to at least match those of the UK GDPR.

Maintaining data security means protecting against a personal data breach.

Security measures include:

- Encryption of all personal financial data
- Clearly specified retention periods.

9. Who do we Share your Personal Data with?

We may share your data with third parties, such as our beneficiaries (individuals) to enable you to provide services directly to them.

We require third parties to respect the security of your data and to treat it in accordance with the law, maintaining standards at least equivalent to the UK GDPR.

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

The following third parties may receive personal information about you for the following purposes:

Recipient	Data disclosed	Purpose of processing
Beneficiaries (individuals)	Contact details, professional experience	To be able to provide services to the beneficiary

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our written instructions.

10. How Long do we Keep your Personal Data for?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Retention periods for personal data will vary according to the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and

whether we can achieve those purposes through other means, and the applicable legal requirements.

You should be aware that supplier documentation such as invoices and remittances are ordinarily retained for six years after the end of the current financial year, which is the statutory limitation period for the retention of accounting records, and then promptly deleted once that period has passed. Supplier contact information will be retained on file for the same time period in case of a query, unless consent is given for us to retain these longer. If we are able to anonymise your personal data so that you can no longer be identified from it, we may use such information without further notice to you.

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. You are responsible for notifying us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

11. What are your Rights in Relation to Personal Data we Process?

Unless subject to an exemption under the UK GDPR, you have a number of rights with respect to your personal data:

- Informed – be informed about our processing of your personal data , which is the purpose of this privacy notice
- Access - request a copy of the data we hold about you and details of what we do with that data (known as a data subject access request)
- Rectification - update or amend the data we hold about you if it is wrong
- Erasure -ask us to remove your personal data from our records
- Restrict processing - ask us to restrict the processing of your personal data
- Data portability - obtain a digital copy of certain personal data
- Object - raise a concern or complaint about the way in which your data is being used
- Automated decision-making and profiling - ask us to explain any automated processing we carry out and the impact of this on you.

You also have the right to withdraw your consent to use of your personal data where we are relying on consent as the lawful basis for processing it.

We may ask for reasonable proof of your identity before providing you with data or carrying out any of the above actions.

12. How can I Exercise my Rights, Complain or Comment?

If you wish to exercise your rights, or if you have a question or complaint, in the first instance please contact a member of the Senior Management Team at the Trust office, using the information in Section 2 above 'Who are we and how can you contact us?'

If you are not happy with the way we respond, you can make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. You can contact the Information Commissioners Office on 0303 123 1113 or via email **https://ico.org.uk/global/contact-us/email/** or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

DOCUMENT REVISION AND SIGN OFF INFORMATION:

Policy:	Suppliers Privacy Notice
Date Policy Written	July 2023
Last Reviewed and Updated	October 2023
Reviewed by	Suzanne Lluch, Finance Director
For next regular review:	October 2026