

# The Thalidomide Trust

## Privacy Notice – beneficiaries

### 1. Background/Introduction

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 [www.thalidomidetrust.org](http://www.thalidomidetrust.org) is a "data controller" for the purposes of data protection legislation. A data controller determines the purposes and means of processing personal data.

Personal data is any information which relates to an individual who can be identified from that information.

Processing includes the collection, recording, storage, use, disclosure or destruction of personal data.

Under the General Data Protection Regulation (GDPR) we are required to provide all data subjects with a privacy notice to inform the subject about why we process personal data and the legal basis for doing so.

This privacy notice applies to beneficiaries as we want to make sure you know about how the Trust uses your information and how we treat your data. The notice may be amended from time to time.

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.

### 2. Data protection principles

GDPR came into force on 25 May 2018 and set out the principles we, as a data controller, must adhere to when processing your personal data.

GDPR principles are as follows:

- *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.

### **3. What personal data we hold on our beneficiaries**

The personal information we hold on you as a beneficiary of the Trust might include:

- name and previous name(s)
- date of birth
- email address
- postal address
- telephone number
- photographic images
- local authority
- bank details
- financial information
- carers and care arrangements
- benefits claimed
- lifestyle details
- insurance arrangements
- vehicles, driving convictions and details of any named drivers
- marital status
- details of family members and close contacts
- equipment and adaptations used
- name of GP
- name of MP
- information you have provided through surveys
- Trust website login details
- information disclosed on NAC conflict of interest declarations

We may also hold special categories of personal data such as information about your health and thalidomide damage. We collect special categories of personal data only if we are permitted to do so by data protection law, and we have additional measures in place to protect this data when sent out electronically.

If you are also a volunteer the personal information we hold on you might also include:

- testimonials
- references
- details of DBS (criminal record) checks
- records of training undertaken to perform the role of volunteer.

#### **4. Why we hold this information**

- to enable us to keep in touch with you
- to support you as a beneficiary of the Trust
- to enable us to make payments to you
- to enable us to verify your existence easily
- for audit purposes
- for funders of the Trust
- for research (only with your consent)
- to plan and assess services offered by the Trust.

#### **5. How we use your personal information**

At the Trust, protecting your data is very important to us and we will only use your data as the law allows us to. The Trust complies with its obligations under (the GDPR) by:

- keeping personal data up to date
- storing and destroying it securely within the data retention guidelines
- not collecting or retaining excessive amounts of data
- protecting personal data from loss, misuse, unauthorised access and disclosure
- ensuring that appropriate technical measures are in place to protect personal data.

The legal bases on which we process your data are:

- Where it is necessary to comply with our legal obligations and/or
- Where it is necessary for the legitimate business of the Trust
- Where we have your consent.

We may pass your personal information to:

- anyone you appoint to act on your behalf
- regulatory bodies
- our external auditors
- beneficiary volunteers (only with your consent). This includes the Trust's Campaign Team where you have agreed to share your contact details with them
- any person/organisation that the Trust contracts or employs to supply services
- any other person or organisation where you have given consent
- or if the law, public duty or our legitimate interest requires the Trust to do so.

Your data will only be kept for as long as necessary. The period of time that we keep each type of information is set out in the Trust's retention policy which is part of its data protection policy. You can also let us know at any time if information the Trust holds about you has changed so we can update it.

## **6. How we store your information**

We place great importance on the security of all personally identifiable information associated with our beneficiaries. All personal financial data is encrypted and we have security measures in place to protect against the loss, misuse and alteration or destruction of personal data under our control. Information is stored by us on password protected computers located in the UK.

We may also store information held securely on paper files.

## **7. How we communicate with you**

In May 2018 we sent all beneficiaries a communication preference form which gave you the right to choose what information we send to you. Whilst some communications at the Trust are essential for beneficiaries to receive (e.g. grant information), there are a number of other communications that you can either 'opt in' or 'opt out' of. You will always have the choice of receiving our communications either via email or post. If you would like to change the way we communicate with you, please contact the Trust office for a new communications preference form or amend your communications preferences on the Trust website.

## **8. Email Communications**

To enable us to tailor communications to your individual needs, we record your communications preferences on our beneficiary database and use an external bulk-mailing system. To do this, we have to share your email address and salutation with an external supplier so we will always ensure that any companies we use for this purpose are GDPR-compliant. This means that if they are in the US, they will have an up to date 'EU-US Privacy Shield Compliance Certificate'. This certificate is recognised and accepted by the ICO (Information Commissioner's Office) as confirming GDPR-compliance

Whenever we send sensitive information by email to you or to an agreed third party (e.g. a doctor we are making a referral to), we will do so using a password protected attachment or via a secure data-link to ensure the data is completely secure.

## **9. Data Breaches**

In the rare event of a possible data breach (a security incident in which sensitive information could be accessed without authorisation), we have robust processes in place to record and investigate this. Any potential data breaches are reported immediately upon discovery to the Finance Director and investigated straight away. If it is confirmed as a data breach and there is a likely risk of harm to an individual as a result, a report will be made within 72 hours to the Information Commissioner and the trustees and any individuals affected will be notified.

## **10. Website**

If you complete a contact form on the Trust website this will include your email address and may also include personal information (for example financial information if you make a payment request or health/accessibility needs if you are booking an event). This information is transferred to the relevant member of staff at the Trust to action and is not retained.

However, if you disclose personal information about yourself on the Thalidomide Community forum on the website, this information will be viewable by other website users.

## **11. Website 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.

The Thalidomide Trust 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.

## **12. Consent**

Under the Data Protection Act 1998, consent was the basis on which most organisations used personal data. Guidance issued in relation to the GDPR has stated that consent should only be relied on as the legal basis for processing where it is freely given, specific, informed and unambiguous. We will not, generally, rely on consent as a legal basis for processing your personal data but in certain circumstances it may be deemed appropriate. Where you provide consent to the Trust to use your data, you will be asked for this when you provide your data to us and you should be aware that you will be able to withdraw your consent at any time.

## **13. Your rights and your personal data**

Unless subject to an exemption (under the GDPR), you have the following rights with respect to your personal data: -

- the right to request a copy of your personal data which the Trust holds about you
- the right to request that the Trust corrects any personal data if it is found to be inaccurate or out of date
- the right to request your personal data is erased where it is no longer necessary for Trust to retain such data
- the right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing

## **14. Any questions?**

If you have any questions or complaints, in the first instance please email [hello@thalidomidetrust.org](mailto:hello@thalidomidetrust.org) or write to the Finance Director at the Trust office.

## **15. Right to contact the Information Commissioner's Office**

You should be aware that you have the right to 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.

<https://ico.org.uk/concerns/>