Tourettes Action

Data Protection Policy

Effective date: 01/01/2018

Review date: 01/01/2020

Approved: Suzanne Dobson, CEO Tourettes Action

Author: Pippa McClounan, Office Manager Tourettes Action

Version Control: 1.2018

CONTENTS

1. Introduction

Tourettes Action controls and processes personal information about its customers, staff and board members. The UK's data protection approach will be amended following the adoption of the General Data Protection Regulation (GDPR) in May 2018. The principles of the new GRPR build on the existing Data Protection Act 1998 (DPA) but the obligations are more extensive.

The Data Protection Act 1998 (the 'Act') covers all personal information that relates to living individuals. These individuals are given rights by the Act. We will not share this information with other organisations without the consent of the individual concerned unless we are required by law to do so.

This Policy will set out what Tourettes Action will do to comply with the GDPR and the existing eight principles in the DPA.

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall only be obtained and further processed for specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose that they are processed.
4. Personal date shall be accurate and kept up to date.
5. Personal data shall not be kept longer than necessary.
6. Personal data shall be processed in line with the rights of the data subject.
7. Personal data must be kept secure.
8. 8. Personal data must not be transferred to a country without adequate protection.

Being fair and understanding our contacts needs

We recognise that communities are made up of people with different needs and values and that those differences are important. We will promote equality of access for everyone and value their diversity. We will work to eliminate discrimination and, in line with the law, we will treat everyone fairly, regardless of age, disability, gender, reassignment, marital status including civil partnerships, pregnancy and maternity, race, religion or belief or sexual orientation. We will ensure that members of all these groups are treated in ways that meet their needs, and that they have equal access to services and/or activities wherever possible. We will promote their inclusion and challenge discrimination against them.

Scope

This policy applies to all employees, board members and others who may be involved in the collection of and processing of personal information on behalf of Tourettes Action and extends to data whether it is held on paper or by electronic means.

Partnership arrangements – where Tourettes Action work in partnership with external service providers, this policy is applicable.

Statement of commitment

Tourettes Action is committed to maintaining high standards of security and confidentiality for information in our custody and control. Safeguarding this information is critical to the successful operation of Tourettes Action. Tourettes Action will treat all information in its care and control with the same degree of security and confidentiality, and this Policy applies to all organisations within Tourettes Action and all of its employees.

2. Objectives

The objectives of this Data Protection Policy are: - To comply with the Data Protection Act 1998 - To comply with the European General Data Protection Regulation, May 2018 - To outline, guide and monitor the coordination of the information, security and data handling procedures in force within Tourettes Action - To promote confidence in Tourettes Action's information, security and data handling procedures - To provide assurances for third parties dealing with Tourettes Action - To provide a benchmark for employees on information, security, confidentiality and data protection issues.

GDPR provides the following rights for individuals (Article 5):

1. The right to be informed
2. The right of access
3. The right of rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Enablers

In order to support these objectives, Tourettes Action will:

- Delegate the responsibility of gathering and disseminating and dealing with issues relating to information, security, the DPA, GDPR and other legislation.
- Ensure that all activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information, security and compliance with GDPR and DPA.
- Ensure that all contracts and service level agreements between any part of Tourettes Action and external third parties (including contract staff), where personal data is processed, make reference to the Act where appropriate.
- Ensure that third parties acting on behalf of Tourettes Action are given access to personal information that is appropriate to the duties they are undertaking and no more.
- Ensure that all staff (including contract staff) and board members understand their responsibilities regarding data protection and information security under the Act.

3. Data Sharing

There are a few occasions where it will be necessary for Tourettes Action to share personal data collected. All contacts are told the nature of the data sharing including what will be shared and the reason for sharing it.

This policy ensures our processes for sharing is legal, how the accuracy of the data will be maintained and what security measures are in place prior to any sharing of information. It also provides the correct parameters of when it is appropriate to share and/ or disclose data. Tourettes Action have appropriate data sharing agreements (DSA) or similar with all parties which are reviewed on a regular basis and recorded on a central DSA log. All decisions to share data are well founded, reflect the current needs of Tourettes Action and compliant under the requirements of the Regulations. The contract confirms that the third party organisation acts a Data Processor for personal data to perform the service or any other obligation. Tourettes Action remain the data controller throughout the contract to deliver the services and have overall control over the purpose for which, and the manner in which, personal data is processed and carry out data protection responsibility for it.

Exemptions

In some circumstances, it may be appropriate to disclose information held by Tourettes Action to specific third parties for example to prevent a criminal offence from being committed, or to prevent the continuation of a criminal offence.

4. Data Retention

Personal data must only be kept for the length of time necessary to perform the process for which it was collected. This applies to both electronic and non-electronic data

Under GDPR a new requirement is the right to be forgotten. Individuals can request deletion of certain types of information about them deleted where one of a number of circumstances apply:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

Disposal

Where personal and confidential information is no longer required, it will be destroyed.

Privacy notice

A privacy notice is published on Tourettes Action's website outlining how we use information collected and a contacts right to request access to personal information.

5. Individuals' rights of access to data (Subject Access Requests (SARs))

Individuals have a right of access to personal information held by Tourettes Action if they are the "data subject" of that information. Requests must be made in writing, signed by the data subject and addressed to the Data Protection Officer. The person requesting the data must complete the Access Request Form providing details of the information required as well as their current address and some form of identification. There is no charge for responding to the request (other than a reasonable administrative fee for providing additional copies of information, unless the request can be said to be "manifestly unfounded or excessive", for example where repetitive requests are made. In those rare cases a data controller may choose to refuse the request entirely, or comply subject to reasonable administrative fee being paid. Timescales for responding to a SAR should be without undue delay or within one month.

Where a SAR is made electronically, the information should also be provided electronically unless the individual requests otherwise. Where possible, Tourettes Action should consider providing individuals with direct and remote access to their data through a secure system. As well as providing copies of the relevant data, Tourettes Action must provide further explanatory information about the way in which the information is used, who it will be shared with, how long it will be kept, and information on the rights to rectification, erasure, and to complain to the ICO.

Someone may ask a third party to obtain the information on their behalf, but they must provide written consent in order to do this.

If a SAR is received directly or indirectly the responsibility for responding will be assigned to the Data Protection Officer. The Data Protection Officer will ensure the SARs are processed

efficiently and in accordance with GDPR; and ensure the documented process has been approved by senior management and made readily available to personnel.

6. Breaches

Tourettes Action has appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. Tourettes Action has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage e.g. through identity theft or confidentiality breach. There are also appropriate mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

Any wilful disregard or intentional breach of the Data Protection Policy by employees shall be regarded as a disciplinary offence and handled within Tourettes Action Disciplinary Procedures. Any wilful disregard or intentional breach of the Data Protection Policy by data processors (and identified data controllers in their own right) acting on Tourettes Action's behalf under contract shall be regarded as a breach of contract and treated as such.

7. Policy promotion and training

The Policy will be made available within Tourettes Action as part of the induction process to all new and temporary employees, board members.

The Policy will be promoted to current employees by requiring acknowledgement and acceptance of its aims and objectives. There will be a continuing series of awareness raising initiatives relating to security and privacy issues by the Data Protection Champions nominated around Tourettes Action in order to ensure that all staff understand their responsibilities under GDPR.

All employees will be provided with education and training where appropriate and will be expected to comply with data protection legislation and adhere to the policies and procedures used to meet the objectives of Tourettes Action's Data Protection Policy.

8. Monitoring and feedback

This policy will be monitored by the Office Manager. It will be reviewed periodically as set out above capturing best practice, customer feedback and any legislative changes.

The Office Manager is responsible for all data compliance and monitors Tourettes Action's approach to Data Protection.

9. Internal Personal Data

Tourettes Action maintains appropriate technical and organisational processes and procedures to safeguard against any unauthorised or unlawful processing of personal data. Data audits are carried out annually to monitor the information we hold on employees, including former employees. For the purposes of HMRC compliance, financial information is held for 3 years and then destroyed. All HR files relating to former employees are kept up to a year after leaving the employment of Tourettes Action.

Glossary of terms

Personal Information – any information that relates to a living individual who can be identified by this data. This includes opinions about the individual and an indication of the intention of Tourettes Action or any other person in respect of the individual.

Data subject – the living individual that the personal data is about.

Data Controller – the company that decides the purpose for and the way in which any personal data is processed. Tourettes Action and certain of its subsidiaries are data controllers.

Data Processor – any company that carries out activities with personal data on behalf of the data controller.

Sensitive Personal Data means personal data consisting of:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or other beliefs
- Whether they are a trade union member
- Their health including physical or mental condition
- Their sexual life
- Criminal proceedings or convictions

Confidential information includes but is not limited to:

- Financial information
- Pricing information
- Administration and information systems

Data can be information, covering both facts and opinions held on:

- Computer
- Paper records
- Any accessible record (e.g. e-mail, electronic device)