Data Protection Policy for the Scottish Transactional Analysis Association

Created by Bob Hunter, Committee Member
Agreed by Board on
Operational From
Reviewed every three years
Next review due

Context & Overview

The Scottish Transactional Analysis Association (STAA) needs to gather and use information about its members and others with whom it has a relationship with or may need to contact.

This policy sets out how the STAA will collect, handle and store this information in order to comply with Data Protection Standards and relevant law.

The policy exists to ensure the STAA:
1) Complies with Data Protection Law and follows good practice
2) Protects staff, members and others from risks associated with the handling of personal information
3) Is open about how it collects, handles and stores personal information
4) Protects itself from the risks associated with unauthorised distribution of personal information

Data Protection Law
The General Data Protection Regulations that came into force on 25th May 2018 describe how organisations, such as the STAA should collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. Personal data must

1) Be gathered in a consensual manner with explicit consent obtained from the individual

2) Be processed fairly and lawfully

3) Be obtained only for specific lawful purposes

4) Be adequate, relevant and not excessive

5) Be accurate and kept up to date

6) Not be held for longer than required

7) Processed appropriately depending on the rights of the individuals on whom information is held

8) Be protected appropriately

9) Not be distributed outside the EEA (European Economic Area)

Scope of the Policy

This policy covers the STAA, including its committee, members, staff and others who may work on its behalf, either paid or unpaid.

The policy applies to all information the STAA holds that relates to identifiable individuals. The STAA will apply this policy to personally identifiable information that lies outside the strict definition of the law. The STAA recognises that as an organisation that works with counsellors and psychotherapists it may hold personally identifiable information that meets the criteria for sensitive personal information. The information the STAA holds will include names, addresses, email addresses, phone numbers and other information that when aggregated will lead to meeting the criteria for either personal information or sensitive personal information.

Data Risks

This policy aims to protect the STAA against

1) Breaches of the GDPR Regulations

2) Breaches of confidentiality

3) Failing to offer appropriate choices to individuals who they hold information on

4) Damage to the reputation of the STAA and the profession of Counselling and Psychotherapy that would ensue from improper use of personally identifiable information

Data Responsibilities

Everyone who works for the STAA, either paid or unpaid has a responsibility to ensure the STAA's use of information complies with this policy and the requirements of GDPR.

The following people have specific responsibilities

1) The Committee have the ultimate responsibility for ensuring compliance with this policy and relevant law.

2) The Chair of the STAA will be the nominated Data Protection Officer. The data protection officer is responsible for

    a) Keeping the committee informed of Data Law and Good Practice

    b) Assessing risks and issues around acquiring, handling and storing personal information. This includes assessing whether the STAA is required to meet the enhanced requirements associated with sensitive personal information

    c) Reviewing Information policies promptly and appropriately

    d) Assessing the need for and arranging for training in Data Protection if it is required

    e) Handling Data Protection queries from STAA committee members, members, staff (paid or unpaid) and also for dealing with requests from individuals to see the information the STAA holds on them.

    f) Ensuring outside bodies who may have access to STAA information have appropriate procedures that meet or exceed the requirements of this policy and relevant law.

    g) Responding to queries from the media.

3) The Data Protection Officer has the responsibility to ensure the STAA's physical and digital systems meet the needs of the organisation and comply with this policy and relevant law. The day to day responsibility for ensuring that information held digitally meets the requirements of this policy and relevant law may be delegated to another member of the STAA committee.

The Information Manager has responsibility for

1) Ensuring physical and/or digital information is held securely, meeting appropriate standards for personally identifiable information.

2) Performing regular checks to ensure data acquisition, handling and storage procedures are appropriate and being followed

3) Ensuring information is backed up appropriately, including backups are secured appropriately and restore procedures work.

4) Ensuring third party systems meet the STAA's Data Protection Policies and relevant law.

The STAA Events Manager has responsibility for

1) Ensuring appropriate data protection statements are made in relevant STAA communications, particularly in emails and social media.

2) Ensuring all marketing materials and campaigns meet relevant data protection standards. This includes ensuring emails do not include the names of all recipients.

3) Ensuring data from campaigns and events is collected, handled and stored in accordance with this policy and relevant law.

4) Ensuring everyone on email mailing lists opts in to receiving email, and can opt out at any time.

5) It is the event manager's responsibility to ensure the STAA mailing lists, including the membership list, are accurate and up to date.

6) It is the Event Managers responsibility to ensure the STAA complies with laws relating to email communication (EU PECD2004 & CAN-Spam). This includes ensuring organisations used by the STAA comply with direct marketing legislation and best practice.

7) It is the Event Managers responsibility to ensure that the STAA complies with Direct Marketing suppression lists

General Guidelines

1) Information is only accessed by STAA members who need it to do paid or unpaid work for the STAA

2) The STAA should ensure that at least one committee member has been trained in Data Protection frameworks

3) Information should not be shared informally

4) If requested the STAA will provide training in Data Protection for committee members and members performing paid or unpaid work involving information acquisition, handling or storage for the STAA

5) The STAA will ensure all personally identifiable information is kept secure by taking appropriate precautions, particularly when personally identifiable information is stored on portable devices and media.

6) Strong passwords should be used on all devices where the STAA's personally identifiable information is handled and/or stored. If the information is in paper form it should be stored in a locked container.

7) Personal data should never be shared with unauthorised people. If there is any uncertainty about whether to share information the issue should be taken up with the Data Protection Officer, Chair of the STAA, or raised at a committee meeting.

8) Information should be reviewed regularly to ensure it is required and up to date. At a minimum this should be done every 2 years

9) Information no longer required should be deleted or disposed of securely. This may involve shredding paper documents. It is important that computer hard drives, disks or media that have been used to store personally identifiable information are rendered unusable before disposal.

10) Reputable cloud computing services may be used for the storage of personally identifiable information. If this information is potentially sensitive the use of the specific Cloud service must be agreed and minuted by the STAA Committee

11) Sensitive personal information must be encrypted if stored digitally. This includes backups

Data Accuracy

The law requires the STAA to do its best to ensure all personal data is accurate and up to date. This means that the STAA must take the following steps

1) Hold data in as few places as possible

2) Take action on a regular basis to check the relevance and accuracy of personally identifiable information.

3) Move toward making it possible for people on whom information is held to be able to update that information via the STAA website.

4) If data is found to be inaccurate it should be deleted. This applies if mail or email is returned/ bounced.

Access Requests

The STAA is required to respond to individuals requesting information the STAA may hold on them. They are entitled to ask

1) what information the STAA holds on them and why

2) For a copy of that information

3) That it be amended if it is not accurate

4) That the information be deleted/destroyed

5) how the STAA is meeting its Data Protection obligations

If an individual contact the STAA and asks one of these questions this is a “Subject Access Request”. This should be made in writing or by email to the Chairperson of the STAA. At the latest the Chair will respond within 14 days after the next committee meeting. The STAA will not charge for responding to Subject Access Requests.

The STAA Chair will always verify the identity of the person making the request before releasing information. How this is done is at the discretion of the STAA Chair.

The STAA may be requested to pass on information in certain statutory circumstances, possibly without the consent or knowledge of the data subject. In this case the Chair of the STAA will verify the identity and legality of the Data Request taking legal opinion if desired. If the request is legal the Chair may act on their own discretion.

Unless the request is made under a statute where disclosure of the request and the response is illegal, the Chair has a duty to inform the data subject and rest of the STAA committee as soon as practicable. The request and Chair’s response must be discussed and minuted at the next committee meeting.

Privacy Statement

The STAA aims to uphold the highest standards of data privacy and security and undertakes

1) not to pass on or sell personal information to other individuals or organisations

2) to ask data subjects to agree to the storage and use of their data, and hold a record of that agreement

3) not to use Personal information for purposes other than that for which it was originally gathered

4) to provide a simple process for data subjects to delete their personal data through unsubscribing.