Data protection policy

as adopted by the AATG Committee on 20 June 2018, revised 5 November 2020

Context and overview

Key details

- Policy prepared by: Michael Connelly
- Approved by AATG Committee: 20 June 2018
- Policy became operational on: 20 June 2018
- Next review date: 1st Committee meeting after AGM

Introduction

The AATG needs to gather and use certain information about individuals.

These can include members, suppliers, business contacts, Newsletter subscribers and other people with whom the AATG has a relationship or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the AATG's data protection standards — and to comply with the "Algemene verordening gegevensbescherming" (AVG) implementing the EU General Data Protection Regulation in the Netherlands.

Why this policy exists

This data protection policy ensures the AATG:

- Complies with data protection law and follows good practice
- Protects the rights of members, Newsletter recipients and other persons
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The EU General Data Protection Regulation, signed into EU law on 25 May 2018, describes how organisations — including the AATG— must 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.

The Data Protection Regulation is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Be processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The Committee of the AATG
- All member and volunteers of the AATG
- Any contractors, suppliers and other people working on behalf of the AATG

It applies to all data that the AATG holds relating to identifiable individuals, even if that information technically falls outside of the GDPR scope. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals, such as the information requested in membership and audition sign-up forms

Data protection risks

This policy helps to protect the AATG from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the AATG uses data relating to them.
- **Reputational damage.** For instance, the AATG could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone involved with the AATG has some responsibility for ensuring data is collected, stored and handled appropriately.

Anyone who handles personal data must ensure that it is handled and processed in line with this policy, the AATG Privacy Statement and data protection principles.

However, these people have key areas of responsibility:

- The **AATG Committee** is ultimately responsible for ensuring that the AATG meets its legal obligations. It is responsible for:
    - Keeping updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions.
    - Dealing with requests from individuals to see the data the AATG holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the AATG's sensitive data.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other members to ensure publicity initiatives abide by data protection principles.
- The **Membership Secretary** (or in his/her absence the Committee) is responsible for:
    - Keeping the membership list current and ensuring that expired members' data is duly removed.
    - Ensuring that membership data is stored and handled in a manner compliant with the GDPR regulations.
    - Maintaining the list of Newsletter subscribers, responding to requests to be removed from the subscribers list and ensuring that the personal information is subsequently deleted.
- The **Webmaster** (or in his/her absence the Committee) is responsible for:
    - Ensuring that, if they are used for storing data (which is not the case at present), the website and any cloud systems meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services the AATG is considering using to store or process data. For instance, cloud computing services.

General guidelines

- The only people able to access data covered by this policy should be those who **need it for their function within the AATG**.
- Data **should not be shared informally**. When access to confidential information is required, members can request it from the Committee.
- **The AATG Committee** will arrange any training needed to help Committee members understand their responsibilities when handling data.
- **Committee members and other members given access to personal data** should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the AATG or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Members **should request help** from the Committee if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Webmaster.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Members should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between members.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **duly protected drives and servers.** If it needs to be uploaded to a **cloud computing service,** this service must be **approved** by the Webmaster, and any **additional exposure of data** must be **approved** by the Committee.
- Data should be **backed up frequently**.
- Extra care is needed when data is stored on laptops or other mobile devices like tablets or smart phones that can be readily lost or stolen.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to the AATG unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, users should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **must be handled in accordance with the Privacy Statement.**

Data accuracy

The law requires the AATG to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the AATG should put into ensuring its accuracy.

It is the responsibility of all users who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Members should not create any unnecessary additional data sets.

- Every effort should **be taken to ensure data is updated.** For instance, by confirming a member's details whenhe or she is contacted about an event or an audition.
- The AATG will make it **easy for data subjects to update the information** the AATG holds about them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a member or subscriber can no longer be reached on their stored telephone number or email address, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by the AATG are entitled to:

- Ask **what information** the AATG holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the AATG is **meeting its data protection obligations**.

If an individual contacts the AATG requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Membership Secretary at membership@aatg.nl

The Membership Secretary will aim to provide the relevant data within 14 days.

The Membership Secretary will always verify the identity of anyone making a subject access request before handing over any information.

Right to be forgotten: the Membership Secretary shall delete all data pertaining to an individual, if so requested by that individual.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the AATG will disclose requested data. However, the Committee will first ensure the request is legitimate.

Providing information

The AATG aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the AATG has a Privacy Statement, setting out how data relating to individuals is used by the AATG. This is posted on the AATG's website or available on request from the Webmaster or Membership Secretary.