Voluntary Action Arun & Chichester

DATA PROTECTION POLICY 2018

1. INTRODUCTION

1.1 VAAC collects and uses certain types of personal information about staff, volunteers, clients and other individuals who come into contact with VAAC.
VAAC may be required by law to collect and use certain types of information to comply with statutory obligations related to employment and this policy is intended to ensure that personal information is dealt with properly and securely in accordance with the General Data Protection Regulation and other related legislation. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulations and other related legislation.
1.2 The GDPR applies to all computerised data and manual files if they come within the definition of a filing system.

2. PERSONAL DATA

2.1 'Personal data' is information that identifies an individual. A sub-set of personal data is known as 'personal sensitive data'. This special category data is information that relates to a persons:

2.1.1. race or ethnic origin;
2.1.2. political opinions;
2.1.3. religious or philosophical beliefs;
2.1.4. trade union membership
2.1.5. physical or mental health;
2.1.6. an individual's sex life or sexual orientation;
2.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person

2.2 Personal sensitive data is given special protection, and additional safeguards apply if this information is to be collected and used.
2.3 VAAC does not intend to seek or hold sensitive personal data about staff, trustees or clients except where it has been notified of the information, or it comes to light via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice.

3. THE DATA PROTECTION PRINCIPLES

3.1 Article 5 of the GDPR sets out six data protection principles which must be followed at all times:

3.1.1. personal data shall be processed fairly, lawfully and in a transparent

manner;

3.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3. personal data shall be adequate, relevant and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for the purpose / those purposes;

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2 In addition to this, VAAC is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

3.3 VAAC is committed to complying with the principles in 3.1 at all times.

This means that we will:

3.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it and will identify who we will share the information with and how long we intend to retain the information;

3.3.2. be responsible for checking the quality and accuracy of the information;

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;

3.3.4. ensure that when information is authorised for disposal it is done in accordance with our disposals policy;

3.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so;

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

3.3.8. report any breaches of the GDPR

4. CONDITIONS FOR PROCESSING

4.1 The individual has given consent that is specific to the particular type of processing activity.

4.2 The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

4.3 The processing is necessary for the performance of a legal obligation to which we

are subject.
4.4 The processing is necessary to protect the vital interests of the individual or another.

5. USE OF PERSONAL DATA BY VAAC

5.1 VAAC collects and uses certain types of personal information about staff, volunteers, clients and other individuals who come into contact with VAAC.
In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3.1 above.
5.2 Any wish to limit or object to use of personal data should be notified to VAAC in writing. If, in the view of VAAC, the objection cannot be maintained, the individual will be given written reasons, why VAAC cannot comply with their request.

Staff, clients and volunteers

5.3 The personal data held about staff, clients and volunteers will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs.
5.4 The data is used to comply with legal obligations placed on VAAC in relation to employment. We may pass information to other regulatory authorities where appropriate. Personal data will also be used when giving references.
5.5 It should be noted that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Other individuals

5.6 VAAC may hold personal information in relation to other individuals who have contact with VAAC, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

6. SECURITY OF PERSONAL DATA

6.1 VAAC will take reasonable steps to ensure that members of staff and volunteers will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under GDPR. VAAC will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

7.1 The following list includes the most usual reasons that VAAC will authorise disclosure of personal data to a third party:

7.1.1. to give a confidential reference relating to a current or former employee;
7.1.2. for the prevention or detection of crime;

7.1.3. for the assessment of any tax or duty;
7.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Council (other than an obligation imposed by contract);
7.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
7.1.6. for the purpose of obtaining legal advice;

7.2. VAAC may receive requests from third parties to disclose personal data it holds about staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or VAAC.

7.3 All requests for the disclosure of personal data must be sent to VAAC, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

8. SUBJECT ACCESS REQUESTS

8.1 Anybody who makes a request to see any personal information held about them by VAAC is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

8.2 A subject access request must be made in writing. VAAC may ask for any further information reasonably required to locate the information.

8.3 All requests will be handled in line with the Subject Access procedural note.

9. OTHER RIGHTS OF INDIVIDUALS

Right to restrict processing

9.1 An individual has the right to object to the processing of their personal data and to block or suppress the processing.

9.2 Where such an objection is made, it must be sent to VAAC who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

9.3 VAAC shall be responsible for notifying the individual of the outcome of their assessment within 20 working days of receipt of the objection.

Right to rectification

9.4 An individual has the right to request the rectification of inaccurate data or incomplete data without undue delay. Where any request for rectification is received, it should be sent to VAAC and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified within 20 days.

9.5 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given details of how to appeal to the Information Commissioner.
9.6 An individual has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

9.7 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- 9.7.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- 9.7.2. where consent is withdrawn and there is no other legal basis for the processing;
- 9.7.3. where an objection has been raised under the right to object, and there is no overriding legitimate interest for continuing the processing;
- 9.7.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- 9.7.5. where the data has to be erased in order to comply with a legal obligation

9.8 VAAC will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to object

9.9 An individual has the right to object to:

- 9.9.1. processing based upon legitimate interests or the performance of a task in the public interest / exercise of official authority (including profiling);
- 9.9.2. direct marketing (including profiling);
- 9.9.3. processing for purposes of scientific / historical research and statistics

9.10 Where such an objection is made, it must be sent to VAAC who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

Right to portability

9.11 If an individual wants to send their personal data to another organisation they have a right to request that VAAC provides their information in a structured, commonly used, and machine readable format. This right is limited to situations where VAAC is

processing the information on the basis of consent or performance of a contract. If a request for this is made, it should be forwarded to VAAC.

10. Zoom Video Conferencing

10.1 Using the Zoom video conferencing app can put your privacy at risk. It is ok to Zoom but you need to take responsibility for ensuring that you have secured the sessions. The Zoom privacy policy includes the right to collect data, store it and share it with third parties such as advertisers. This does not just include your name, location and usage information, but also "the content contained in cloud recordings and instant messages, files (and) whiteboards…….shared while using the service."

10.2 The following actions should be taken to ensure security:

- 10.2.1 a public meeting link is public, so don't share it with anyone you do not trust;
- 10.2.2 same goes for your personal meeting ID. This is essentially a personal phone number that people can "drop in" on at any time. Set up a password for participants to verify their entry before entering;

10.3 When you are in the meeting before entering:

- 10.3.1 manage screen sharing by ensuring you are the person in control of the meeting. To do this, click on " Who Can Share" and confirm that "Host" is the only button clicked;
- 10.3.2 manage participants by ensuring only signed-in participants can join the call. This way you know who people are if they are behaving badly;
- 10.3.3 set two-factor authentication, remove unwanted or disruptive participants, disable video for participants and disable private chat;
- 10.3.4 say something if you see something. You can report unwanted activity, harassment and cyberattacks to Zoom directly.

11. BREACH OF ANY REQUIREMENT OF THE GDPR

11.1 Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to VAAC.

Once notified, VAAC shall assess:

- 11.1.1. the extent of the breach;
- 11.1.2. the risks to the data subjects as a consequence of the breach;
- 11.1.3. any security measures in place that will protect the information;
- 11.1.4 any measures that can be taken immediately to mitigate the risk to the individuals

11.2 Unless VAAC concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Charity.

11.3 The Information Commissioner shall be told:

- 11.3.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

11.3.2. the contact point for any enquiries;
11.3.3. the likely consequences of the breach;
11.3.4. the measures proposed or already taken to address the breach

11.4 If the breach is likely to result in a risk to the affected individuals then VAAC shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected indiviuals.

11.5 Data subjects shall be told:

11.5.1. the nature of the breach;
11.5.2. who to contact with any questions;
11.5.3. measures taken to mitigate any risks

11.6 VAAC shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by VAAC and a decision made about implementation of those recommendations.