

Data Protection Policy: September 2025

1. Introduction

VAAC collects and uses certain types of personal information about employees, Trustees, charities, and other individuals who contact us. We may be required by law to collect and use certain types of information to comply with statutory obligations related to employment. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation ((EU) 2016/679) ("The GDPR") and other related legislation.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR and other related legislation.

The GDPR applies to all computerised data and manual files if they come within the definition of a filing system.

This policy is not part of your employment contract, and VAAC may amend it at anytime.

2. Compliance and compliance officers

VAAC is required to comply with Data Protection Laws. Our directors, employees, workers, contractors and others in similar capacities must comply with these laws. You must ensure that you read and understand this policy to know what you must and must not do and what is required from you in handling and using any Personal Data for you and VAAC to comply with the Data Protection Laws.

If you do not comply with this policy, we may take disciplinary action against you.

We have appointed the CEO as our Data Protection Officer (referred to in this policy as the DPO), who oversees VAAC's compliance with Data Protection Laws.

You should contact the DPO if you have any questions or concerns about data protection, data protection laws, this policy, or any breach of the laws or this policy.

This policy also indicates specific situations when you must contact the DPO, for example, when there is a Personal Data breach before you use or handle data in a new way or when you receive any request from an individual exercising any of their rights under the Data Protection Laws.

3. The Data Protection Principles

Article 5 of the GDPR sets out six data protection principles which must always be followed:

Personal Data must be processed fairly, lawfully and in a transparent manner.

Personal Data must be collected for specific, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.

Personal Data must be adequate, relevant, and limited to what is necessary for the purpose(s) it is being processed.

Personal Data must be accurate and, where necessary, kept up to date.

Personal Data processed for any purpose(s) shall be kept only as long as it is necessary for that purpose / those purposes.
report any breaches of the GDPR.

4. Personal Data

Any information from which a living individual (a Data Subject) can be identified. It does not apply to information that has been anonymised. Personal Data can come in many forms: at its simplest, it may be a name, address and telephone number, but it can include a wide range of matters such as an individual's opinion or preferences. Under GDPR, an IP address is also considered to be Personal Data.

A sub-set of personal data is known as 'personal sensitive data'. This special category data is information that relates to a person's:

- race or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade union membership.
- physical or mental health.
- an individual's sex life or sexual orientation.
- genetic or biometric data to uniquely identify a natural person.

Personal sensitive data is given special protection, and additional safeguards apply if this information is to be collected and used.

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.

5. Conditions for Processing

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

The processing is necessary for the performance of a contract to which the individual is a party or is necessary for taking steps to enter into a contract with the individual at their request.

The processing is necessary to perform a legal obligation to which we are subject.

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

6. Use of Personal Data by VAAC

VAAC collects and uses certain types of personal information about staff, Trustees, volunteers, residents, and other individuals who come into contact with us. In each case, personal data must be treated according to the data protection principles outlined in the paragraph above.

Any wish to limit or object to the 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 we cannot comply with their request.

Personal data held about staff, Trustees, and volunteers will include contact details, employment history, career progression information, DBS checks, and photographs.

The data is used to comply with VAAC's legal obligations concerning employment. We may pass information to other regulatory authorities where appropriate. Personal data will also be used when giving references.

It should be noted that information about disciplinary action may be kept longer than the duration of the sanction. Although the sanction is treated as “spent” once the period has expired, the details of the incident may need to be kept longer.

VAAC may hold personal information about other individuals who have contact with us, such as volunteers and guests. Such information shall be stored only in accordance with data protection principles and kept for as long as necessary.

7. Security of Personal Data

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

8. Disclosure of Personal Data to Third Parties

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

- to give a confidential reference relating to a current or former employee.
- for the prevention or detection of crime.
- for the assessment of any tax or duty.
- where it is necessary to exercise a right or obligation conferred or imposed by law upon VAAC (other than an obligation imposed by a contract).
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings).
- for the purpose of obtaining legal advice.

VAAC may receive requests from third parties to disclose personal data it holds about staff or other individuals. This information will only generally be disclosed if one of the specific exemptions under data protection legislation allows disclosure or where necessary for the legitimate interests of the individual concerned or VAAC.

All requests for the disclosure of personal data must be sent to VAAC, which will review and decide whether to make the disclosure. Before making any disclosure, reasonable steps must be taken to verify the identity of the third party.

9. Subject Access Requests

Anybody who requests 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.

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

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

10. Other Rights of Individuals

Right to Restrict Processing

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

Where such an objection is made, it must be sent to VAAC, which 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 to establish, exercise or defend legal proceedings.

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

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.

Where there is a dispute about 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.

An individual also has a right to have any incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to Erasure

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

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

VAAC will decide regarding any application for the erasure of personal data and will balance the request against the exemptions provided in the law. Where a decision is made to erase the data, which 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

An individual has the right to object to:

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

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 to establish, exercise or defend legal proceedings.

Right to Portability

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

11. Personal Data Breaches

A personal data breach is where a breach of security occurs that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Although it is impossible to provide an exhaustive list of what constitutes a personal data breach, examples include:

- an email containing Personal Data is sent to the wrong person.
- papers or records containing Personal Data being stolen or left in a public place.
- access to Personal Data by an unauthorised staff member or a third party.
- access to our systems by a hacker or similar authorised access.

All breaches of the GDPR, including a breach of any of the data protection principles, shall be reported to the DPO as soon as it is discovered.

The DPO will investigate and deal with the personal data breach. The DPO will decide whether the personal data breach needs to be reported to the ICO and/or relevant Data Subjects. If the DPO decides that the personal data breach needs to be reported to the ICO, they will do so within 72 hours after VAAC becomes aware of the breach.

12. Automated Decision Making and Profiling

Under Data Protection Laws, Automated Decision Making (including Profiling) that has a legal or similar effect on the Data Subject is prohibited unless VAAC meets one of three specific grounds that lift the restriction. These are:

- necessary for the entry into or performance of a contract.
- authorised by domestic law applicable to the controller.
- based on the individual's explicit consent.

Examples of Automated Decision Making include a recruitment test that uses algorithms and other criteria, and it must be solely automated with no human involvement in the decision.

Before undertaking any Automated Decision Making, including Profiling, you must contact the DPO, who will be able to assist you in ensuring compliance with the Data Protection Laws.

If VAAC carries out Automated Decision Making that does not produce legal or similar effects, then it is not prohibited from doing this. However, we must still comply with the Data Protection Laws.

13. Direct Marketing

Any marketing to customers and other business contacts must be carried out strictly in compliance with Data Protection Laws and laws relating to marketing.

The marketing laws are complex and depend on how the marketing is to be conducted (e.g. letter, telephone or email) and who the intended recipients are (e.g. individuals (including sole traders and partners of partnerships) or companies).

Before undertaking any direct marketing, you must contact the DPO, who can assist you in ensuring compliance with the marketing and Data Protection Laws.

Data Subjects can opt out of receiving direct marketing at any time. If you receive a request objecting to direct marketing or a Data Subject opts out/unsubscribes from receiving it, you should promptly ensure this is noted on our database. Under Data Protection Laws, rather than deleting their details from our database, we can retain just enough information to record their marketing preferences to ensure that no further marketing is sent to them in the future.

Version Control

Version Number	Date of Update	Amendments
4.0	23/06/2025	Updated Format