

---

## 1. Data protection principles

AVP Ireland is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

---

## 2. General provisions

- a. This policy applies to all personal data processed by AVP Ireland
- b. The board of directors shall take responsibility for AVP Ireland’s ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.

---

### **3. Lawful, fair and transparent processing**

- a. To ensure its processing of data is lawful, fair and transparent, AVP Ireland shall maintain a Register of Systems - see Annex 1
- b. The Register of Systems shall be reviewed at least annually.
- c. Individuals have the right to access their personal data and any such requests made to AVP Ireland shall be dealt with in a timely manner.

---

### **4. Lawful purposes**

- a. All data processed by AVP Ireland must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
- b. AVP Ireland shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the AVP Ireland's systems.

---

### **5. Data minimisation**

- a. AVP Ireland shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

---

### **6. Accuracy**

- a. AVP Ireland shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

---

### **7. Archiving / removal**

- a. To ensure that personal data is kept for no longer than necessary, AVP Ireland shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

---

## 8. Security

- a. AVP Ireland shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be in place.

---

## 9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, AVP Ireland shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Data Commissioner.

ADOPTED ON July 2018

Board members

Coordinator

# Annex 1

## REGISTER OF SYSTEMS

---

### Introduction

In accordance with the General Data Protection Regulation which came into force on 25 May 2018, this document sets out how AVP Ireland collects, uses and manages the personal data of its volunteers under the following headings:

- The data we collect and in what way
- How the data are stored and who has access to them
- Sharing the data
- Purpose for which the data are used
- Data removal and archiving

---

### The data we collect and in what way

#### Outside volunteers:

When applying for volunteering with AVP, individuals send by email to the coordinator their CV, application for prison clearance (with their names, date of birth, address for the past 10 years and court history). They fill out a Google form with their contact details (email, postal address and phone number).

Subsequently applicants are invited to subscribe themselves to our newsletter generated via Mailchimp by providing their name and email address to the Mailchimp's database.

When volunteers apply for Garda Vetting, AVP Ireland receives a vetting disclosure by email from the Volunteer Centre (South Dublin County).

#### Prison based volunteers:

In prison AVP Ireland only collects the names of participants in a workshop, with their consent.

All data is collected on a the lawful basis of consent.

---

### How the data is stored and who has access to it

Only the coordinator of AVP Ireland has access to all the data.

The coordinator's computer is encrypted and password protected.

The file storing personal data is passport protected and backed up on a Tresorit Cloud: the datacenter is located in Europe and the data is encrypted and not accessible to Tresorit staff.

In case of emergency, the board of Directors has the password to access the computer and the files and AVP International webmaster can access the emails.

#### Outside volunteers:

All data is stored on the coordinator's computer with a back up system on the Tresorit cloud.

The data includes

- CVs
- Application forms from the Google drive (they are deleted from the Google drive as soon as the application is completed)
- Applications for prison clearances until they are fully processed by IPS
- Approvals for prison clearance as long as they are active
- Vetting disclosures for three years

CVs, applications for prison clearance, approvals for prison clearance and vetting disclosures received by email are destroyed from the email's files as soon as they are processed and securely stored on the computer's file.

Hard copies of prison clearances received by post before May 2018 are stored in a file in the attic of the coordinator's house and destroyed when they have expired.

All volunteers are invited to fill out a Google form to consent to the different aspects of our register of systems regarding data protection.

#### Inmate volunteers:

A database of participants in workshops is maintained on a spreadsheet stored on the coordinator's computer, when consents from participants have been gathered.

Consents from inmates are gathered at the end of a workshop, scanned and stored on the coordinator's computer (Annex 2).

The lead outside volunteer who has access to the names of inside participants in a workshop has signed a confidentiality agreement (Annex 3).

---

## Sharing the data

### Outside volunteers:

Application for prison clearance are shared with Irish Prison Services.

Data exchanged by emails or via Google forms are temporarily and indirectly shared with Google.

Contact details of volunteers can be shared between them only if they have given consent.

### Inmate volunteers:

The lead outside facilitator of a workshop has access to the names of participants that he/she will share with the coordinator after the workshop. The list is destroyed when the names are processed by the coordinator.

The complete data set is shared solely as described above. The complete data set will not be shared with any third party unless legally obliged to do so.

---

## Purpose for which the data are used

The data are processed on the basis of consent.

### Outside volunteers:

Contact details are used to share information about the activities of AVP Ireland and to organise the workshops.

CV and motivation statements are used to scan volunteers and ensure adequacy.

### Inmate volunteers:

The database of participants in a workshop allows to re-issue certificates on request if they are lost.

---

## Data removal and archiving

Data can be modified, removed and destroyed at any time if a volunteer requests it.

Volunteers can opt out from the mailing list when they want.

Data from active volunteers is kept as long as they are active. Data from inactive volunteers are kept for a maximum of 3 years after they cease being active.

Database of participants are kept for a period of 7 years.

ADOPTED ON July 2018

AVP Ireland Directors

AVP Ireland Coordinator



## Annex 3



Quaker House  
Stocking Lane  
Rathfarnham  
Dublin 16  
Ph: 0851512582  
*Charity number: 14196*

## Confidentiality agreement

I \_\_\_\_\_, agree with the following statements:

I understand that I will be in contact with confidential information such as names of inmates taking part in AVP workshops.

As a condition of my volunteer work with AVP Ireland, I hereby undertake to keep in strict confidence any information and data regarding any participants or co-facilitators during a workshop.

I have read and am in agreement with the AVP GDPR policy which is available on the AVP website.

When acting as a lead outside facilitator, once a workshop is complete I will forward the list of names of participants to the coordinator, by email, and make sure to destroy/delete the email from my mail box and the list when the coordinator has answered.

Print name

Signature

Dated