# AVS Privacy Policy

| Last Amendment: | Review Date: | Approved by: | Next Review: |
|---|---|---|---|
| May 2020 | February 2022 | AVS ARMC | February 2025 |

## 1. Summary

The purpose of this policy is to establish requirements for the way in which Agriculture Victoria Services Pty Ltd (AVS) collects, stores, uses and discloses personal and health information in accordance with the Privacy and Data Protection Act 2014 (Vic) (PDP Act) and the Health Records Act 2001 (Vic).

## 2. Scope

This policy applies to all personal and health information AVS collects, stores, uses and discloses to perform its business functions and activities. This policy applies to all AVS directors, employees, contractors and third parties whose personal information may be held by AVS.

## 3. Policy Statement

This policy supports AVS' need to collect, store and use personal and health information, and the right of the individual to privacy. It ensures that AVS can collect personal and health information necessary for its services and functions, while recognising the right of individuals to have their information handled in ways they would reasonably expect and in accordance with the law.

Personal and health information is collected and used by AVS to:

- plan, fund, implement, monitor, regulate and evaluate AVS services and functions
- fulfil statutory and other legal functions and duties
- comply with reporting requirements,
- investigate incidents and/or defend any legal claims against AVS or its employees, and
- Support employee health and wellbeing.

AVS is subject to the Information Privacy Principles and Health Privacy Principles set out in the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 as minimum standards when dealing with personal information.

These principles regulate the way AVS collects, stores, provides access to, uses, discloses and corrects personal information. Subject to certain exceptions, AVS must not do or refrain from doing, an act, or engage in a practice that contravenes an Information Privacy Principle.

## 4. Policy Requirements

This policy provides information on:

- the circumstances under which AVS collects, stores, uses and discloses personal information
- how AVS manages collected information
- the circumstances allowing AVS to disclose personal information to organisations and/or individuals outside of Victoria
- how an individual may access their personal information or seek the correction of such information, and
- how an individual may complain about a possible misuse of their personal information by AVS, and how AVS will handle their complaint.

## 5. Principles

AVS directors, employees and other workplace participants must ensure the information privacy requirements are adhered to when collecting, using, storing and disclosing personal information:

### 5.1 Use and Disclosure

AVS must only collect personal and/or health information if the information is necessary to perform its functions or activities. AVS will only use that information for the primary purpose for which it is collected, unless:

- use or disclosure is for a related secondary purpose and is reasonably expected

- the individual has provided consent
- use or disclosure is reasonably necessary to carry out a law enforcement function, or
- use or disclosure is required, permitted or authorised by law.

In limited circumstances, AVS is required or authorised by law to release information to other government agencies and law enforcement bodies to lessen or prevent:

- a serious and imminent threat to an individual's life, health, safety or welfare, or
- a serious threat to public health, public safety or public welfare.

## 5.2 Collection

AVS must only collect personal and or health information if that information is necessary for its functions or activities and:

- AVS has gained consent from the individual, or
- collection of that information is necessary to prevent or lessen a serious or imminent threat to the well-being of an individual.

Where the personal and/or health information of an individual is collected, reasonable steps should be taken to ensure that the individual is aware of:

- the purposes for which the information is being collected
- the identity of AVS and how to contact it
- the fact that the individual is able to gain access to the information
- to whom that information will be disclosed
- the legislation which requires that information to be collected, and
- the main consequences for the individual if all or part of the information is not provided to AVS.

Where health information about an individual is collected, AVS:

- must not collect health information about an individual in an unreasonably intrusive way, and
- must only collect health information about an individual from someone else where the information is necessary

If health information about an individual is given in confidence by someone else (not to be communicated to the individual to whom it relates) AVS must:

- confirm with the provider that the health information is to remain confidential
- take reasonable steps to record the health information is given in confidence and is to remain confidential
- record the health information only if it is relevant to the care of the individual, and
- take reasonable steps to ensure that the information is accurate and not misleading.

## 5.3 Data Quality

AVS values information as an important resource. Accordingly, AVS should take reasonable steps to ensure that all personal and/or health information it collects, uses or discloses is accurate, complete, up to date.

Generally, AVS relies upon individuals to provide accurate and complete information and to advise AVS if the information collected has recently changed.

## 5.4 Data Security

AVS is guided by the principle that all information is well governed and managed.

AVS seeks to protect personal and/or health information from misuse, loss or unauthorised access, modification or disclosure.

AVS will take reasonable steps to securely destroy or de-identify personal and/or health information when it is no longer needed in accordance with the Public Records Act 1973.

## 5.5 Openness

AVS will maintain and make accessible clearly expressed policy on its management of personal and health information.

On request by an individual, AVS should take reasonable steps to let the person know:

- what sort of personal and/or health information it holds
- for what purposes such information has been collected, and
- how it collects, holds, uses and discloses that information.

## 5.6 Accessing and Correction

Individuals have the right to access and correct their personal and/or health information held by AVS.

In most cases, requests for access will be administered in accordance with the access and correction provisions of the Information Privacy Principles particularly requests that may affect the privacy of another individual or where the personal or health information relates to a commercial activity.

AVS may deal with requests to access and correct information informally if the request is straightforward and only relates to the individual.

An individual may request formal access or correction to their personal information by contacting AVS' Company Secretary or HR Manager.

AVS must provide written reasons for refusal of access to correct health information.

## 5.7 Unique Identifiers

AVS does not assign, use or disclose unique identifiers to individuals unless it is necessary to enable it to carry out its functions efficiently.

## 5.8 Anonymity

Where lawful and practicable, individuals have the option of not identifying themselves when entering into transactions with AVS.

## 5.9 Transborder Data Flows

If an individual's personal and/or health information travels outside Victoria, their privacy protection should travel with it.

AVS should only transfer personal and/or health information about an individual to someone who is outside Victoria if:

- the individual consents to the transfer
- AVS reasonably believes that the recipient of the information is subject to a law binding scheme or contract which effectively upholds principles for fair handling of the information which are substantially similar to the Information Privacy Principles
- the transfer is necessary for the performance of a contract between the individual and AVS, or for the implementation of pre-contractual measures taken in response to the individual's request, or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the department and a third party.

## 5.10 Sensitive Information

AVS must only collect sensitive information in limited circumstances. For example, AVS may collect sensitive information if the individual has consented or if the collection is required by law.

## 5.11 Exceptions

Victorian privacy law stipulates certain situations where AVS does not need to comply with or where an exception is permissible under the Information Privacy Principles or Health Privacy Principles.

Consultation is recommended to determine whether the particular facts require an approval, and if so, whose approval is required.

Should certain situations arise, exceptions to the privacy principles should be referred to the AVS Company Secretary.

### 5.12 Complaints

Where an individual believes that their personal and/or health information has been mishandled or misused by AVS they may lodge a complaint with the AVS Company Secretary.

AVS should be efficient and fair when investigating the complaint and aim to respond within approximately 30 days.

## 6. Responsibilities

AVS directors, employees and other workplace participants are responsible for ensuring they meet their obligations under this policy and for reporting any breaches to the AVS Company Secretary.

This policy will be reviewed and updated when required to account for new laws, technology and processes.

The review process will be conducted by the AVS Company Secretary, with oversight from the AVS Chief Executive Officer and the Audit & Risk Management Committee.

The Accountable Officer for this policy is the AVS Company Secretary. The Accountable Officer is responsible for:

- development of the policy
- implementing any supporting protocols, processes and guidelines, and
- ongoing monitoring of compliance with this policy.

## 7. Breach of Policy

Suspected breaches of this policy must be reported to the Company Secretary and will be investigated by AVS as required. AVS employees who are found to be in breach of this policy will be managed in accordance with relevant AVS policies, as well as any relevant legislation or regulations. A breach of this policy may lead to action under the AVS Managing Misconduct Policy which may result in outcomes up to and including dismissal.

## 8. European Union (EU) Privacy Provisions - EU General Data Protection Regulation (GDPR)

If you are an individual based in the EU the GDPR may apply to personal data processed by AVS relating to you. If the GDPR does apply AVS will comply with the privacy policy outlined in Appendix 3.

## 9. Policy basis

- *Privacy and Data Protection Act 2014* (Vic)
- *Health Records Act 2001* (Vic)
- Office of the Commissioner for Privacy and Data Protection (CPDP)
- Office of the Australian Information Commissioner (OAIC)
- *Public Records Act 1973*
- *EU General Data Protection Regulation (GDPR)*

## 10. Policy Review and Approval

This policy is reviewed in accordance with the requirements of the *AVS Policy Development & Review Policy*.

This policy is a Category B Policy and reviews are approved by the AVS ARMC.

This policy aligns with the *Privacy and Data Protection Act (2014) (Vic)* the *Health Records Act 2001 (Vic)* and the Department of Jobs Precincts & Regions Privacy Policy as at February 2019.

### Document History and Version Control

| Version | Date Approved | Author | Approved by | Brief Description |
|---|---|---|---|---|
| 4.0/2022 | February 2022 | Co Sec | AVS ARMC | Recognition of Health Records Act 2001. Aligned with DJPR. |
| 3.0/2020 | May 2020 | Co Sec | AVS ARMC | Aligned with **European Union (EU) privacy provisions** |
| 2.0/2019 | Feb 2019 | Co Sec | AVS ARMC | Policy mirrors current DJPR and Privacy & Data Protection Act 2014 |
| 1.0 | 2015-2016 | Co Sec | AVS Board | Policy aligned with Privacy Act 1988 requirements |

# 11. Appendix 1 - Protecting personal information

## 11.1 What is Information Privacy and why is it important to protect?

Information privacy is the right of individuals to determine for themselves when, how, and to what extent their personal information is shared with others.

The way AVS and its contracted service providers collect, use and handle personal information is governed by the Information Privacy Principles. These principles are set out in the *Privacy and Data Protection Act 2014 (Vic)*.

Protecting privacy is not only important because it is required by law, but it also ensures that the rights of an individual are protected. A failure to uphold privacy rights can lead to privacy breaches and complaints being made against AVS.

## 11.2 What is personal information?

Personal information may include, but is not limited to:

- Name, address, birth date, telephone number
- Age, sex, marital status
- Finger prints and other biometrics
- Educational, financial, criminal or employment history, and
- An image in a photograph or voice in a recording.

### How are privacy rights protected?

An individual has the right to:

- Know why AVS is asking for personal information and what they are going to do with it
- Ask to see their personal information and request corrections if necessary, and
- Make a complaint if they believe their personal information has been mishandled.

## 11.3 What are the Information Privacy Principles (IPPs)?

Victoria's Privacy and Data Protection Act (PDPA) outlines ten Information Privacy Principles (IPPs) that govern the way that an organisation collects and handles personal information to protect information privacy rights.

The information privacy principles relate to:

- IPP 1 - Collection
- IPP 2 - Use and Disclosure
- IPP 3 - Data Quality
- IPP 4 - Data Security
- IPP 5 - Openness
- IPP 6 - Access and Correction
- IPP 7 - Unique Identifiers
- IPP 8 - Anonymity
- IPP 9 - Transborder Data Flows
- IPP 10 - Sensitive Information

## 11.4 How do I identify a privacy breach?

A privacy breach occurs when there is a failure to comply with any one or more of the Information Privacy Principles (IPPs) contained within the PDPA. Some of the most common privacy breaches occur when personal information of an individual is inappropriately accessed, disclosed or mishandled.

If you suspect there has been a possible privacy breach, please contact the AVS Company Secretary.

## 11.5 How do I prevent a privacy breach?

Some common ways to prevent a privacy breach include:

- Ensuring a Collection and Disclosure Statement is in place when collecting personal information so that the individual is aware how their personal information will be used and disclosed
- Conducting a Privacy Impact Assessment for any new project that involves personal information
- Ensuring Security controls are in place to restrict access to personal information (e.g., password encryption, user access control etc)
- Ensuring protective markings have been applied to information to alert users to the presence of personal information. For more information read the Information Classification Handling Policy.

## 11.6 What to do when you have a privacy breach?

In the first instance contact the AVS Company Secretary to seek advice.

Depending on the severity of the breach, there are four key steps you can undertake to manage a privacy breach (or suspected breach):

1. Contain the breach and conduct a preliminary assessment
2. Evaluate the risks associated with the breach
3. Remediate and notify (and other steps to mitigate harm)
4. Review the cause of the breach and the organisation's response and take steps to improve practices and lessen the likelihood of future breaches

## 11.7 What is a Privacy Impact Assessment?

A privacy impact assessment (PIA) is a method used when planning and managing any project that involves personal information. A PIA should be undertaken before a project commences and throughout the development and implementation of a project in order to identify any potential privacy risks so that risks can be mitigated. The Office of the Victorian Information Commissioner (OVIC) has a PIA template for you to read, download and complete.

## 11.8 What is a Collection & Disclosure Statement?

A Collection and Disclosure Statement is required when you are undertaking any activity or project that requires the collection, use and disclosure of personal information of an individual.

When drafting a collection and disclosure statement/disclaimer, you should advise the individual of the following:

1. The purpose of collection
2. The type of information being collected
3. Whether personal information is being collected (as defined within the Privacy and Data Protection Act)
4. What will be done with that information
5. Whether it will be provided to a third party/parties, and what they will do with that information
6. How AVS will store that information
7. Whether the information will be released to the public
8. What method the information may be aggregated, provided to third parties or published.

AVS also collects, uses and discloses personal information about its people. Read its Collection and Disclosure Statement to learn more about how AVS protects the privacy of our people.

Further information is available from the OVIC website.

For assistance in drafting such a statement, please contact the AVS Company Secretary.

### 11.9 What are my responsibilities?

All AVS staff are responsible for collecting and handling personal information appropriately.

They should:

- Be familiar with the AVS privacy policy and collection and disclosure statement
- Consider the potential or actual uses of personal information when undertaking projects or activities and identify any risks through a privacy impact assessment
- Seek assistance if required
- Undertake the online privacy training.

### 11.10 Online Privacy Training

The Office of the Victorian Information Commissioner (OVIC) has developed an online privacy training module that explores the obligations of Victorian Public-Sector organisations under Part 3 of the PDPA.

To access the online module visit the Knowledge Hub**.**

## 12. Appendix 2 - Collection and Disclosure Statement – Personal Information collected from AVS staff

The following collection and disclosure statement outlines how AVS collects, uses, discloses and manages the personal information it collects about its staff.

AVS recognises that the personal information it collects is important to you and often of a highly sensitive nature. Accordingly, AVS has adopted privacy compliance standards which ensure your personal information is protected.

The *Victorian Privacy and Data Protection Act* 2014 governs the collection, use and disclosure of your personal information.

### 12.1 Collecting your personal information

In its capacity as an employer, AVS collects a range of personal information. Wherever possible, this information is collected from you directly and it is AVS' aim to collect it lawfully, fairly and without undue intrusion.

Personal information that may be collected by AVS, where appropriate, includes: contact information, health and medical information, private interest declaration, education, training and licences, court orders, police declarations, payroll data and history, conditions of employment, leave history, work performance data, WorkCover information and general work-related information.

In some circumstances, personal information will be collected and stored by external organisations such as ADP Payroll. If these circumstances arise, AVS will take all reasonable steps to obtain the consent from you for such collection.

### 12.2 Why AVS collects your personal information

The primary purpose of collection of personal information is to facilitate your employment, your entitlements, your remuneration and your health and wellbeing. If you do not provide complete and accurate information as requested, AVS may not be able to effectively manage your employment.

### 12.3 Disclosing your personal information

Generally, AVS uses information only for the purpose for which it was collected or a related purpose you would reasonably expect (in the case of sensitive information a directly related purpose) unless you have consented for another specific use.

In some circumstances, AVS is required or authorised by law to release information to other government agencies, law enforcement bodies or to prevent serious and imminent threat to an individual's life, health, safety or welfare. In this context, such agencies could include the Australian Tax Office, the Australian Bureau of Statistics, the Victorian WorkCover Authority, the Electoral Commission, Centrelink, your nominated banking institution, your nominated superannuation fund, AVS authorised medical and rehabilitation providers.

Various information attributes about you and your role collected via the DJPR Employee Self Service (ESS) system will be made available to all DJPR staff via the ESS and the department's internal intranet. Information that may be available to all DEDJTR staff include your position details, work location, work contact details, work mobile phone number, key responsibilities and your photo if you choose to upload your photo within the ESS system.

### 12.4 Other important information

AVS will seek wherever possible to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date. In many instances AVS relies upon you to provide accurate and complete information and to advise AVS should your circumstances change over time.

AVS seeks to protect your personal information from misuse, loss, unauthorised access, modification or disclosure and securely destroys or de-identifies personal information when it is no longer needed for any purpose.

In circumstances where personal information is collected and stored by external organisations AVS's contractual obligations ensure compliance with privacy and security standards.

AVS staff have the right to request access to their personnel file through the HR Manager. This right is restated under the Information Privacy Principles, whereby you can access personal information that AVS holds about you on your personnel file by contacting the HR Manager.

## 13. Appendix 3 - EU General Data Protection Regulation ("GDPR")

The GDPR may apply to personal data processed by AVS relating to an individual in the EU while AVS carries out its role commercialising Intellectual Property and negotiating commercial agreements in which AVS may process personal data in order to:

- plan, fund, implement, monitor, regulate and evaluate AVS services and functions
- fulfil statutory and other legal functions and duties
- comply with reporting requirements, and
- investigate incidents and/or defend any legal claims against AVS or its employees.

### 13.1 GDPR Principles

The GDPR sets out seven key principles for the management of personal data:

- Lawfulness, fairness and transparency - Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- Purpose limitation - Data shall be 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
- Data minimisation - Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accuracy - Data shall be 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
- Storage limitation - **Data shall be 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**
- Integrity and confidentiality (security) - Data shall be 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
- Accountability - The controller shall be responsible for, and be able to demonstrate, compliance with the principles

These principles are followed by AVS in the processing of any personal data of EU individuals which may be covered by the GDPR.

If AVS obtains personal data from individuals in the EU to which the GDPR applies it will comply with the requirements of the GDPR and the following provisions apply to any such data;

- Lawfulness, fairness and transparency - Data will be processed lawfully, fairly and in a transparent manner.
- Purpose limitation - Data will be collected for specified, explicit and legitimate purposes to enable AVS to carry out its function to commercialise intellectual property and will not be further processed in a manner that is incompatible with that purpose.
- Data minimisation - Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accuracy - Data will be accurate and kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate will be erased or rectified without delay
- Storage limitation - Data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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
- Integrity and confidentiality - Data will be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures
- Accountability - AVS will be responsible for, and be able to demonstrate, compliance with the principles.

## 13.2 Data Protection Officer

The Company Secretary is AVS'Data Protection Officer whose job it is to oversee AVS' data protection compliance. You can contact AVS' Data Protection Officer by sending:

- an email to: The Company Secretary
- a letter to: Data Protection Officer - Agriculture Victoria Services Pty. Ltd. (AVS), AgriBio Centre for AgriBioscience, 5 Ring Road, Bundoora, Victoria, 3083, Australia

## 13.3 Mandatory data breach notification requirements (Article 33)

The AVS Data Protection Officer will report any reportable data breaches to the appropriate supervisory authority within 72 hours of the breach occurring, upon AVS staff following the AVS EU GDPR internal procedure.