# Privacy Policy

| Document Number | Version Number | Information Classification |
|---|---|---|
| GP 252-1 (11) | 11.0 | Public Information |
| **Approved by** | | **Date** |
| Chief People & Information Officer | | 13/12/2024 |
| **Document Owner** | | **Incumbent** |
| Chief People & Information Officer | | Michael Smith |

**Document History**

| Date | Version | Version Details | Author | Reviewer/s |
|---|---|---|---|---|
| 13/12/2024 | 11 | Updated to reflect Maxima's current environment and align with new governance/procedures | Manager, Cyber Risk and Governance | Head of ICT Services |

## Contents





© Maxima Training Group (AUST) Ltd
Information Classification: Public Information

# 1. Purpose

This Privacy Policy outlines Maxima's commitment to protecting the privacy of people's personal information. It ensures compliance with the *Privacy Act 1988*, the *Australian Privacy Principles (APPs)*, Australian Government's Information Security Manual, ISO 27001:2022, and the *Spam Act 2003*. The policy supports all of Maxima's business operations, and service delivery across all services.

# 2. Scope

This policy applies to all personal information that Maxima collects, uses, stores, and shares, including data from clients, employees, contractors, third-party providers, trainees and apprentices. It encompasses all methods of data handling, whether electronic or physical, and applies to all Maxima Sites, employees and associated personnel regardless of where they work.

# 3. Principles

Maxima is committed to:

- **Transparency**: Clearly communicating how personal information is collected, used, and disclosed.
- **Security**: Implementing robust security measures to protect personal information.
- **Access and Correction**: Allowing individuals to access and correct their personal information.
- **Accountability**: Ensuring compliance with relevant legal and regulatory obligations and that Maxima's people handling personal information are aware of their responsibilities for protecting the privacy of people's personal information.

# 4. Policy Requirements

This section outlines the specific procedures and actions Maxima undertakes to ensure compliance with privacy principles. This section provides detailed guidance on how personal information is collected, managed, disclosed, accessed, and corrected. It also describes the processes for handling complaints related to privacy concerns. These requirements are designed to ensure transparency and accountability in Maxima's data handling practices and to protect the privacy of individuals, particularly those involved in Disability Employment Services (DES) and the National Disability Insurance Scheme (NDIS).

## 4.1 Collection of Personal Information

4.1.1 Personal information must be collected only when necessary for Maxima's functions or activities.

4.1.2 Collection methods include online forms, in-person interactions, and third-party sources.

4.1.3 Individuals must be informed about the collection, the collection and use purpose and consent obtained when required.

## 4.2 Collection Methods

Personal information is collected through various methods depending on the nature of the interaction:

- **Jobseekers**: Collected via application forms, Employment Services Assessments (ESAt), medical reports, and feedback during placement activities.
- **Customers**: Collected during business interactions and service provision.
- **Training Program Participants**: Collected through enrolment forms and related documentation.
- **Referees**: Collected during the verification of jobseeker references.
- **NDIS Participants**: Collected during service delivery, evaluation, and monitoring.


GP 252-1 (11) 13/12/2024
© Maxima Training Group (AUST) Ltd
Information Classification: Public Information

## 4.3 Use and Disclosure of Personal Information

4.3.1 Personal information must be used primarily for the purpose for which it was collected.

4.3.2 It may be used for related purposes reasonably expected by the individual or with the individual's consent.

4.3.3 Information may be disclosed to third-party providers, government agencies, and other entities as required by law or to fulfill contractual obligations.

## 4.4 Privacy Impact Assessments (PIAs)

4.4.1 PIAs are conducted for projects and initiatives involving personal information to identify and mitigate privacy risks.

## 4.5 Disclosure of Personal Information

4.5.1 Information is disclosed only for the purposes it was collected or as required by law.

4.5.2 Disclosures may include sharing with government entities, contracted service providers, and other authorised parties.

4.5.3 Information sharing is conducted in accordance with relevant legal and regulatory requirements.

## 4.6 Access and Correction

4.6.1 Individuals have the right to request access to their personal information and seek correction of any inaccuracies.

4.6.2 Requests can be made to Maxima's Chief People & Information Officer, in writing via PO Box 164, Brooklyn Park SA 5032.

4.6.3 Maxima will verify the identity of the requester and provide the information, unless restricted by law.

4.6.4 Maxima will take reasonable steps to update the information and notify third parties where applicable.

## 4.7 Information Management, Security and Storage

4.7.1 Maxima employs a range of security measures, including encryption, access controls, and secure storage solutions for Personal information.

4.7.2 Information is regularly updated to ensure accuracy and relevance.

4.7.3 Information is de-identified or destroyed when no longer required, in accordance with legal and contractual obligations.

4.7.4 Third Party Contracts include clauses ensuring compliance with Maxima's privacy standards.

4.7.5 Regular third-party risk assessments (TPRAs) are conducted to evaluate their handling of personal information.

## 4.8 Training and Awareness

4.8.1 All Maxima employees receive regular training on data handling and privacy obligations.

## 4.9 Data Breach Response

4.9.1 Maxima has a Data Breach Procedure to manage data breaches promptly and effectively should they occur, including notifying:

- Affected individuals; and
- The Office of the Australian Information Commissioner (OAIC) as required by the *Notifiable Data Breaches (NDB)* scheme.

## 4.10 Compliance with the *Spam Act 2003*


GP 252-1 (11) 13/12/2024
© Maxima Training Group (AUST) Ltd
Information Classification: Public Information

Maxima will:

4.10.1 Obtain explicit consent before sending any electronic messages.

4.10.2 Ensure messages clearly identify Maxima as the sender.

4.10.3 Include an easy-to-use opt-out mechanism in each message.

4.10.4 Prohibit practices such as sending electronic communications without prior explicit consent or using misleading subject lines.

### 4.11 Complaints and Enquiries

4.11.1 Privacy complaints and enquiries can be directed to Maxima's Privacy Officer, PO Box 164, Brooklyn Park SA 5032.

4.11.2 Complaints will be acknowledged, investigated, and resolved in a timely manner, with guidance provided for further action if necessary.

## 5. Roles and Responsibilities

The effective implementation of this policy requires the commitment of all personnel. Key roles and associated responsibilities are summarised in the table below:

| Role | Responsibilities |
|---|---|
| Executive Leadership Team | • Provide strategic oversight and allocate resources to ensure the effective implementation of the privacy policy.<br>• Review privacy risks and incidents at an organisational level.<br>• Promote a culture of privacy compliance and accountability across all departments. |
| Chief People & Information Officer | • Act as the primary owner of the privacy policy, responsible for ensuring its alignment with legal and regulatory requirements.<br>• Oversee privacy risk management and compliance activities, including internal audits.<br>• Act as the point of escalation for unresolved privacy complaints and incidents.<br>• Ensure timely review, updates, and communication of the privacy policy. |
| Cyber Risk and Governance Manager | • Develop, implement, and maintain procedures related to privacy, including Privacy Impact Assessments (PIAs), data breach responses, and training programs.<br>• Conduct regular risk assessments to identify and mitigate privacy risks.<br>• Liaise with third-party providers to ensure compliance with Maxima's privacy standards through Third-Party Risk Assessments (TPRAs).<br>• Monitor legislative and regulatory updates to ensure ongoing compliance. |
| Risk and Compliance Committee | • Review privacy-related KPIs and ensure alignment with organisational risk management frameworks.<br>• Provide recommendations for policy updates and improvements based on compliance metrics and incidents.<br>• Support the development of training and awareness initiatives to address privacy risks. |
| Line Managers | • Communicate the privacy policy and related procedures to their teams.<br>• Ensure team members complete required privacy training and comply with policy requirements.<br>• Report any potential privacy risks or incidents to the Cyber Risk and Governance Manager. |
| All Employees and Contractors | • Comply with the privacy policy and associated procedures in their daily activities.<br>• Protect personal information they handle from unauthorised access, disclosure, or loss. |


GP 252-1 (11) 13/12/2024
© Maxima Training Group (AUST) Ltd
Information Classification: Public Information

| | |
|---|---|
| | • Report privacy concerns, risks, or breaches promptly to their line manager or the Cyber Risk and Governance Manager. |
| Third-Party Providers | • Ensure compliance with Maxima's privacy standards as outlined in contractual agreements.<br>• Implement appropriate technical and organisational measures to safeguard personal information.<br>• Cooperate with Maxima during Third-Party Risk Assessments (TPRAs) and audits. |

## 6. Communication

6.1 Internally, this policy will be communicated through Maxima's Intranet and included in onboarding materials for new staff.

6.2 Externally, this policy will be made available via Maxima's Website.

6.3 Regular updates and training will ensure continued awareness, including being communicated to all relevant stakeholders.

## 7. Measurement and Evaluation

7.1 The effectiveness of this policy will be measured through KPIs reported quarterly to the Risk and Compliance Committee.

7.2 The policy will be reviewed biennially or when significant changes occur.

## 8. Compliance

8.1 Exceptions to policy requirements must be requested through Maxima's Chief People & Information Officer.

8.2 Non-compliance may result in disciplinary action for employees or termination of services for third parties.

## 9. Definitions

**Complaint Management Procedure**: A process for handling complaints related to the management of personal information to ensure they are addressed promptly and effectively.

**Data Breach**: A security incident in which personal information is accessed, disclosed, or destroyed without authorisation, resulting in a compromise of confidentiality, integrity, or availability.

**Data Processor**: Any individual or company processing personal information on behalf of Maxima.

**Disability Employment Services (DES)**: Services provided to support individuals with disabilities in finding and maintaining employment.

**Electronic Messages**: Any communication sent over digital platforms, including emails, SMS, and social media.

**Explicit Consent**: Agreement obtained through affirmative action by an individual authorising Maxima to send electronic communications.

**National Disability Insurance Scheme (NDIS):** A support scheme for Australians with a disability, providing funding for services and support to achieve personal goals and improve quality of life.

**Notifiable Data Breaches (NDB) scheme**: A legal requirement under the *Privacy Act 1988* mandating organisations to notify individuals and the OAIC about data breaches that are likely to result in serious harm.

**OAIC:** Office of the Australian Information Commissioner.


GP 252-1 (11) 13/12/2024
© Maxima Training Group (AUST) Ltd
Information Classification: Public Information

**Personal Information**: is defined under the *Privacy Act 1988* as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether it is recorded in a material form or not. Examples of personal information include:

- Name, address, email address, and phone number
- Date of birth
- Financial details
- Employment details
- Photographs or videos

**Privacy Impact Assessment (PIA):** A process to identify and mitigate privacy risks associated with projects involving personal information.

**Sensitive Information**: is a subset of personal information that is afforded a higher level of protection under the *Privacy Act 1988*. It includes information or opinions about an individual's:

- Racial or ethnic origin
- Political opinions or membership of a political association
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a professional or trade association or trade union
- Sexual orientation or practices
- Criminal record

It also includes:

- Health information
- Genetic information
- Biometric information used for automated biometric verification or identification
- Biometric templates

**Third-Party Risk Assessments (TPRAs):** Evaluations conducted to ensure third-party providers comply with Maxima's privacy standards and handle personal information appropriately.

## 10. Key Associated Documents

- Confidentiality Procedure (GPR 252-1)
- Data Breach Procedure (GPR 150-23)
- Information Classification Scheme (GPR 218-6)
- Information Sharing Policy (GP 252-2)
- Privacy Impact Assessment Procedure (GPR 252-4)
- Risk Management Policy (GP 101-1)
- Spam Act Policy (GP 512)

## 11. References

- *Privacy Act 1988 (Cwlth)*
- *Spam Act 2003 (Cwlth)*
- *Australian Privacy Principles (APPs)*
- ISO 27001:2002


GP 252-1 (11) 13/12/2024
© Maxima Training Group (AUST) Ltd
Information Classification: Public Information

## 12. Appendices

- Nil


GP 252-1 (11) 13/12/2024
© Maxima Training Group (AUST) Ltd
Information Classification: Public Information