Monkey Software Data Security Policy
Updated 27/09/2024

1. Introduction

Monkey Software is committed to ensuring the security and protection of the personal data that we process, and to provide a compliant and consistent approach to data protection. This policy outlines our approach to data security and the measures we have implemented to protect the data of our users.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to Optomate.Net and eCatalogue.com.au data. It covers all data processed within the Optomate.Net and eCatalogue.com.au applications, hosted on the Microsoft Azure platform.

3. Data Protection Principles

We adhere to the following data protection principles:

- Lawfulness, Fairness, and Transparency: Data is processed lawfully, fairly, and in a transparent manner.

- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Data Minimisation: Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

- Accuracy: Data is accurate and, where necessary, kept up to date.

- Storage Limitation: Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.
  Specifically, Optomate.Net patient data is retained for a period of 7 years, or when the patient reaches the age of 25, at which point the patient and all related medical and transaction data is purged. Additionally, patient registration data is purged on a monthly basis where today's date is greater than the appointment date plus 30 days.

- Integrity and Confidentiality: Data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

4. Security Measures

To ensure the security of data processed within Optomate.Net and eCatalogue.com.au, we have implemented the following measures:

- Access Control: Access to data is restricted to authorised personnel only. Role-based access controls are in place to ensure that users only have access to data necessary for their role.

- Encryption: Data is encrypted both in transit and at rest using industry-standard encryption protocols.

- Regular Audits: Regular security audits are conducted to identify and address potential vulnerabilities.

- Incident Response: A robust incident response plan is in place to address any data breaches or security incidents promptly.

- Training: Regular training is provided to all employees on data security best practices and their responsibilities under this policy.

5. Data Subject Rights

We respect the rights of data subjects and ensure they can exercise their rights under applicable data protection laws. These rights include:

- Right to Access: Data subjects can request access to their personal data.

- Right to Rectification: Data subjects can request correction of inaccurate or incomplete data.

- Right to Erasure: Data subjects can request deletion of their personal data.

- Right to Restrict Processing: Data subjects can request restriction of processing of their personal data.

- Right to Data Portability: Data subjects can request the transfer of their personal data to another service provider.

- Right to Object: Data subjects can object to the processing of their personal data.

- Right to Consent: We will not share personal data unless the owner of that data expressly permits us to do so.

6. Compliance and Monitoring

We regularly review and update our data security practices to ensure compliance with applicable laws and regulations. Monitoring and auditing processes are in place to ensure adherence to this policy.

7. Contact Information

If you have any questions or concerns about this Data Security Policy, please contact us at 1300 650 295 or NZ 0800 666 539 or email support@monkeysoftware.com.au.