Privacy & Data Protection Policy

Overarching Policy for the Protection of Personal Information

Governance & Ownership

Policy Owner: Key Account Manager (Head of Operations)
Executive Sponsor: Company Director
Reviewer: Key Account Manager (Head of Operations)
Legal Review: External Legal Counsel (if applicable)
Approved By: Company Director

Version & Review Control

Version	Effective Date	Review Frequency	Next Review Date
1.0	March 2026	Annually	March 2027

Document Classification

Classification: Internal Use Only

Confidentiality Statement

This policy is the property of Genesys Creative Systems. It is intended for internal use only and may not be distributed, reproduced, or disclosed to any external party without the prior written approval of the Head of Operations or Company Director.

Introduction

Genesys Creative Systems is committed to protecting personal information and ensuring that it is processed lawfully, fairly, and securely. This policy sets out the principles and requirements for the collection, use, storage, and protection of personal data in accordance with applicable data protection legislation, including POPIA. It applies to all employees, contractors, and third parties involved in the processing of personal information.

Purpose & Scope

The purpose of this policy is to ensure that Genesys Creative Systems processes personal information lawfully, fairly, and securely in accordance with the Protection of Personal Information Act (POPIA) and applicable data protection requirements.

This policy establishes principles and safeguards to protect the confidentiality, integrity, and availability of personal information processed by Genesys Creative Systems in the course of its operations and service delivery.

Scope includes:

- All personal information processed by Genesys Creative Systems as part of its operations and services
- All employees, contractors, and third-party service providers who process personal information on behalf of the organisation
- All systems, platforms, applications, and cloud services used to store or process personal information

Definitions

- Personal Information (PI): Information relating to an identifiable, living natural person, and where applicable, an identifiable juristic person, as defined in POPIA
- Responsible Party: The entity that determines the purpose and means of processing personal information
- Operator: A person or organisation that processes personal information on behalf of a Responsible Party
- Data Subject: The individual to whom the personal information relates
- Processing: Any operation performed on personal information, including collection, storage, use, dissemination, or deletion
- Consent: Any voluntary, specific, and informed expression of will by which a data subject agrees to the processing of personal information.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA (Act 4 of 2013): Sections 8–25, Section 18, Sections 19–22, Section 14
- Consumer Protection Act (CPA)

- Electronic Communications & Transactions Act (ECT Act)
- King IV Corporate Governance Code

Best Practice References:

- ISO/IEC 27701 (Privacy Information Management)
- NIST Privacy Framework
- GDPR (international privacy benchmark)
- NIS2 Directive (EU 2022/2555)

Policy Requirements

Lawful, Fair & Transparent Processing

Personal information must be processed lawfully, fairly, and transparently in accordance with applicable data protection requirements.

- Personal information must only be collected for specific, lawful, and clearly defined purposes
- Where consent is relied upon, it must be explicit, informed, and freely given
- Where Genesys Creative Systems processes personal information as an Operator, processing must be governed by a written agreement with the Responsible Party

Data Minimisation & Purpose Limitation

Only the minimum amount of personal information necessary for the intended purpose must be collected and processed.

- Personal information must only be used for the purpose for which it was collected
- Only the minimum amount of personal information necessary must be collected and processed
- Personal information must not be retained or used beyond its intended purpose

Data Accuracy

Reasonable steps must be taken to ensure that personal information is accurate, complete, and kept up to date where necessary. Inaccurate or outdated information must be corrected or removed where identified.

Security Safeguards

Appropriate technical and organisational measures must be implemented to protect personal information.

- Access to personal information must be restricted based on the principle of least privilege
- Security controls such as encryption, authentication (including MFA where applicable), and logging should be implemented where feasible

- Systems processing personal information must be secured and monitored
- Third-party providers must implement appropriate security controls
- Personal information must be protected against unauthorised access, loss, or disclosure

Data Subject Rights

Genesys Creative Systems must respect and support the rights of data subjects in accordance with applicable data protection requirements.

- Data subjects must be able to request access to their personal information
- Data subjects must be able to request correction or deletion of inaccurate or unnecessary information
- Requests must be handled in a timely and appropriate manner

Data Retention & Disposal

Personal information must not be retained for longer than necessary and must be securely disposed of when no longer required.

- Retention must be aligned to business, legal, and regulatory requirements
- Personal information must be securely deleted or destroyed when no longer required
- This policy must be read in conjunction with the Data Retention and Disposal Policy

Cross-Border Data Transfers

Where personal information is transferred or stored outside South Africa:

- Appropriate safeguards must be in place to ensure the protection of personal information
- Data must only be transferred to jurisdictions or service providers that provide an adequate level of protection
- Third-party providers must be contractually required to protect personal information

Third-Party Processing (Operators)

Where third parties process personal information on behalf of Genesys Creative Systems:

- Appropriate contractual agreements must be in place
- Third parties must implement appropriate security and data protection measures
- Processing must be limited to defined purposes
- Third parties must notify Genesys Creative Systems of any data breaches in a timely manner

Breach Notification

Personal data breaches must be managed in accordance with legal and regulatory requirements.

- Breaches must be identified, investigated, and contained promptly, in accordance with the Incident Response Policy
- Where required, the Information Regulator and affected data subjects must be notified as soon as reasonably possible
- Additional notifications and updates may be provided as more information becomes available

Roles & Responsibilities

- Company Director: Ultimate accountability for information security governance, risk management, and compliance.
- Key Account Manager (Head of Operations): Responsible for the day-to-day implementation, enforcement, and coordination of information security controls and policies. Ensures that security practices are embedded in business operations.
- Technology Service Providers (Internal or External): Responsible for the technical implementation, configuration, maintenance, and support of systems and security controls, including cloud platforms, hosted environments, and custom-developed applications. This includes managing security configurations, applying updates, and supporting incident response where required.
- Employees & Contractors: Must comply with all information security policies, procedures, and controls. Responsible for protecting company information, using systems securely, and reporting any suspected security incidents.
- Third-Party Service Providers: Must comply with Genesys Creative Systems' security requirements as defined in contracts and agreements. Responsible for protecting any systems or data they access or process on behalf of the organisation.

Exceptions

Exceptions to this policy must be documented, justified, and approved by the Head of Operations. All exceptions shall be recorded in the Risk Register. High-risk exceptions require escalation to the Company Director.

Consequences of Non-Compliance

Non-compliance with this policy may result in disciplinary action (employees), termination of contract (vendors/contractors), and potential reporting to regulatory authorities under POPIA.

Monitoring & Enforcement

Genesys Creative Systems must monitor compliance with this policy to ensure that personal information is processed in accordance with applicable data protection requirements.

- Personal data processing activities should be reviewed periodically to ensure alignment with defined purposes and legal requirements
- Data handling practices should be monitored to ensure that personal information is collected, used, and protected appropriately

- Requests from data subjects (e.g. access, correction, deletion) should be tracked and managed in a timely manner
- Security incidents involving personal information must be identified, investigated, and managed in accordance with incident response processes
- Where third parties process personal information, their compliance should be monitored through ongoing engagement and contractual oversight

Where non-compliance or risks are identified:

- Appropriate corrective actions must be implemented to address gaps in data protection practices
- Processing activities may be restricted or adjusted where necessary to mitigate risk
- Significant issues may be escalated to management for oversight and resolution

Related Policies

This policy should be read in conjunction with:

- Information Security Policy
- Data Classification Standard
- Data Retention and Disposal Policy
- Data Security and Encryption Policy
- Access Control Policy
- Incident Response Policy

Acknowledgement

All employees and contractors are required to:

- Read and understand this policy
- Comply with its requirements
- Acknowledge adherence as part of onboarding and ongoing employment obligations

This policy is made available via the organisation's internal document repository.

Oversight & Review

This policy will be reviewed annually by the Head of Operations and updated as required to reflect changes in regulation, technology, or organisational needs.

Document Control & Version History

Version	Date	Owner	Reviewer	Approved By	Next Review Date
1.0	March 2026	Key Account Manager (Head of Operations)	Key Account Manager (Head of Operations)	Company Director	March 2027

Version History

Version	Date	Description of Changes	Author	Reviewer
1.0	March 2026	Initial version aligned with POPIA and best practices (ISO, NIST)	Key Account Manager (Head of Operations)	Key Account Manager (Head of Operations)