HUGHMARI
LANDGOED

POPIA
COMPLIANCE MANUAL
& PRIVACY POLICY

HUGHMARI LANDGOED CC

Farm Frischgewaagd, Trichardt 2300, Mpumalanga
+27 82 666 0893 | info@hmlandgoed.co.za
www.hmlandgoed.co.za

Version 1.0 | Effective date: 25 June 2026

Prepared as a practical POPIA compliance framework for the business.

Document Status and Completion Notes

Important

This document is a practical POPIA compliance manual and privacy policy. It does not replace Hughmari Landgoed CC's separate PAIA Manual, the registration of its Information Officer with the Information Regulator, or advice from a suitably qualified legal professional. The manual must be formally approved, kept updated and reviewed when business, legal, system or processing changes occur.

Document item	Details
Responsible party	Hughmari Landgoed CC
Physical address	Farm Frischgewaagd, Trichardt 2300, Mpumalanga
Telephone	+27 82 666 0893
Email	info@hmlandgoed.co.za
Website	https://hmlandgoed.co.za/
VAT registration number	4640257848
CC registration number	2010/065144/23
Information Officer	Robbie Becker, Information Officer
Version	1.0
Effective date	25 June 2026
Review date	At least annually, and sooner after a material business, legal, system or processing change

Before this manual is signed

- Confirm that Robbie Becker, Information Officer, is registered with the Information Regulator.
- Confirm the current list of staff members, service providers and operators that handle personal information.
- Confirm the actual systems used for orders, website forms, WhatsApp, email, accounting, cloud storage, photographs and backups.
- Confirm the retention periods against the business's accounting, tax, employment and contractual obligations.
- Approve the manual in writing and make the public privacy notice available on the website or on request.

Contents

- 1. Purpose, status and scope
- 2. Legal and regulatory framework
- 3. Accountability and governance
- 4. Personal information processed by the business
- 5. Lawful and responsible processing
- 6. Customer orders, website enquiries and WhatsApp
- 7. Direct marketing and customer updates
- 8. Photo shoots, photographs and children
- 9. Security safeguards and operators

- 10. Security compromise response plan
- 11. Data subject rights and request handling
- 12. Retention, archiving and secure destruction
- 13. Complaints, training, monitoring and review
- Annexure A - Personal information request form
- Annexure B - Marketing consent and opt-out record
- Annexure C - Photograph and media consent form
- Annexure D - Security incident and breach log
- Approval and reference sources

1. Purpose, Status and Scope

This manual sets out how Hughmari Landgoed CC ("Hughmari", "the business", "we", "us" or "our") protects personal information in the course of operating a pomegranate farm, selling farm products, responding to customer enquiries, maintaining customer relationships and arranging seasonal photo shoots on the farm.

It is intended to support practical compliance with the Protection of Personal Information Act 4 of 2013 (POPIA), the applicable regulations and guidance issued by the Information Regulator. It also contains a public-facing privacy notice that may be provided to customers, website visitors, suppliers, photographers, photo shoot participants and other data subjects.

1.1 Scope

This manual applies to personal information processed in paper or electronic form by the business, its members, employees, temporary workers, contractors and service providers. It covers information collected through the website, email, telephone calls, WhatsApp, order forms, invoices, photo shoot bookings, consent forms, marketing lists, supplier records, employment records and related business systems.

1.2 Policy principles

- Collect only information that is reasonably required for a clear and lawful purpose.
- Be open with people about what is collected, why it is needed and how it will be used.
- Keep personal information accurate, relevant, secure and no longer than necessary.
- Respect requests for access, correction, deletion, objection and withdrawal of consent.
- Use photographs, customer contact details and marketing lists responsibly and with appropriate consent.
- Respond promptly and transparently when personal information may have been compromised.

2. Legal and Regulatory Framework

POPIA establishes eight conditions for the lawful processing of personal information: accountability; processing limitation; purpose specification; further processing limitation; information quality; openness; security safeguards; and data subject participation. Hughmari applies these conditions throughout the personal information life cycle.

This manual must be read with the Protection of Personal Information Act 4 of 2013, the Regulations Relating to the Protection of Personal Information, the Promotion of Access to Information Act 2 of 2000 (PAIA), the Consumer Protection Act 68 of 2008 where applicable, tax and accounting record-keeping requirements, employment laws, and current guidance issued by the Information Regulator.

Separate PAIA requirement
A POPIA compliance manual is not a substitute for the PAIA Manual required from a private body where applicable. The Information Officer details used in this manual should match the details registered with the Information Regulator and published in the PAIA Manual.

3. Accountability and Governance

3.1 Responsible party

Hughmari Landgoed CC is the responsible party for personal information where it determines why and how the information is processed.

3.2 Information Officer

The Information Officer is responsible for encouraging compliance with POPIA, dealing with requests from data subjects, working with the Information Regulator, maintaining this manual, overseeing privacy impact assessments and ensuring that appropriate safeguards and internal procedures are implemented.

Role	Name / details	Core responsibilities
Information Officer	Robbie Becker, Information Officer	POPIA and PAIA oversight; registration; complaints; requests; security compromise reporting; policy approval and review.
Deputy Information Officer	No Deputy Information Officer designated.	Not applicable. No Deputy Information Officer has been appointed.
Staff and contractors	All persons who handle information	Follow this manual, maintain confidentiality, use approved systems and report incidents immediately.
Operators	Service providers that process information for Hughmari	Process only under written instructions, preserve confidentiality and maintain appropriate security safeguards.

3.3 Privacy by design

Before introducing a new form, app, mailing list, booking process, camera system, online service or supplier that will handle personal information, the business should consider what information is needed, the lawful reason for processing it, who will have access, where it will be stored, how long it will be retained, and what risks could arise. Higher-risk processing should be documented in a personal information impact assessment.

4. Personal Information Processed by the Business

The exact information processed depends on the relationship and the service requested. The following inventory is intended to reflect the ordinary activities of the business and must be updated when operations change.

Data subject	Typical personal information	Purpose
Customers and prospective customers	Name, telephone number, email address, delivery or collection details, order details, communications, invoice details and payment status.	Answer enquiries, process and fulfil orders, arrange collection or delivery, issue invoices, provide support and maintain business records.
Website visitors	Information submitted through forms, IP address and basic technical or cookie data where enabled by the website platform.	Operate and secure the website, respond to enquiries, understand website performance and prevent abuse.

Data subject	Typical personal information	Purpose
Photo shoot clients and participants	Names, contact details, preferred dates, package details, number of participants, photographer details, messages, photographs or video where consent is provided.	Plan and administer sessions, communicate arrangements, protect farm operations, process payment and use approved images for marketing.
Children participating in photo shoots	Name or age where necessary, images and consent details of the parent, guardian or other competent person.	Administer the session and use images only where authorised and appropriate.
Photographers and creative suppliers	Name, contact details, business information, booking details, correspondence and payment records.	Coordinate access, services, payments, safety and contractual arrangements.
Suppliers and service providers	Contact people, telephone numbers, email addresses, banking or payment details, invoices, contracts and compliance records.	Procurement, payments, supplier management, legal compliance and business administration.
Employees, casual workers and applicants	Identity and contact details, employment history, qualifications, payroll and tax information, bank details, emergency contacts, attendance and performance records.	Recruitment, employment administration, payroll, safety, legal obligations and workforce management.
Visitors and complainants	Name, contact details, visit or complaint information and related correspondence.	Farm access, safety, incident handling, complaints and legal record keeping.

4.1 Special personal information

The business does not intentionally collect special personal information unless it is necessary and lawful. Health or emergency information may be processed where voluntarily supplied for safety reasons, employment obligations or a specific photo shoot requirement. Such information must receive additional protection and restricted access.

4.2 Information about children

Information about a child must be processed only with a lawful basis and, where required, the consent of a parent, guardian or other competent person. Images of children must not be published for marketing merely because they took part in a family photo shoot. Separate, clear and recorded permission must be obtained.

5. Lawful and Responsible Processing

5.1 Lawful justification

Before processing personal information, Hughmari must identify a lawful justification. Depending on the circumstances, processing may be based on the data subject's consent, steps necessary to conclude or perform a contract, compliance with a legal obligation, protection of a legitimate interest of the data subject, performance of a public-law duty, or the legitimate interests of the business or a third party, provided those interests do not unfairly override the data subject's rights.

5.2 Minimality and collection

- Information should normally be collected directly from the person concerned.
- Forms and conversations must request only information that is adequate, relevant and not excessive for the stated purpose.
- Optional fields should be clearly identified as optional.
- Personal information obtained for one purpose must not be reused incompatibly without a lawful basis and appropriate notice.

5.3 Openness and collection notice

At or before collection, the business should provide a concise notice explaining the identity and contact details of the responsible party, what information is collected, whether supply is mandatory or voluntary, the purpose and lawful basis, possible recipients, retention, rights of the data subject, and how to complain. The notice may be provided on the website, in a form, by email, by WhatsApp or verbally where appropriate, with a record kept when consent is relied upon.

5.4 Information quality

Reasonable steps must be taken to keep information complete, accurate, not misleading and updated where necessary. Customers and suppliers should be able to correct their contact details, and marketing lists should be cleaned when messages fail or a recipient opts out.

6. Customer Orders, Website Enquiries and WhatsApp

6.1 Orders and enquiries

Contact information received through the website, WhatsApp, email or telephone may be used to answer the enquiry, confirm availability, provide pricing, process an order, arrange collection or delivery, issue an invoice and provide reasonable after-sales assistance. It should not automatically be added to a marketing list unless there is an appropriate basis and the person has been informed.

6.2 Website and cookies

The website should display a clear privacy notice and identify any cookies or analytics tools in use. Non-essential tracking or advertising technologies should not be enabled without an appropriate consent mechanism. The business should keep its website platform, plugins and administrative accounts updated and secured.

6.3 WhatsApp and messaging

WhatsApp is used as a practical customer communication channel. Staff must send messages only from approved business accounts or devices, avoid sharing customer contact details in groups without permission, and refrain from storing unnecessary sensitive information in chat histories. Orders, consent and important instructions should be transferred to an approved business record where necessary rather than being left only in a private device chat.

Customer privacy notice - short version
When you contact Hughmari Landgoed, we use the details you provide to answer your enquiry, process your order or booking, communicate arrangements and meet our legal and accounting obligations. We do not sell your personal information. You may contact info@hmlandgoed.co.za to ask about, correct or object to our use of your information.

7. Direct Marketing and Customer Updates

Direct marketing includes promotional messages sent by email, SMS, WhatsApp or other electronic communication. Unsolicited electronic direct marketing must be handled in accordance with section 69 of POPIA, the current regulations and the Information Regulator's guidance.

7.1 Rules for electronic marketing

- Do not send unsolicited electronic marketing to a person unless valid prior consent exists or the limited existing-customer exception applies.

- When consent is required, use the current prescribed Form 4 or an equivalent process that records the required information and preferred communication method.
- A prospective recipient who has not previously withheld consent may be contacted only once for the purpose of requesting consent.
- Every marketing message must identify Hughmari and provide a simple, free method to stop future messages.
- Opt-outs, objections and withheld consent must be recorded and honoured promptly across all marketing lists.
- Consent records must show who consented, when, for what products or services, and through which communication channel.

7.2 Existing customers

Where permitted by law, existing customer details may be used to market Hughmari's own similar products or services if the details were obtained in connection with a sale, the customer was given a reasonable opportunity to object when the details were collected, and every subsequent message includes an opportunity to object. This exception must be applied narrowly and documented.

Recommended opt-out wording
Hughmari Landgoed sent this message. Reply STOP or contact info@hmlandgoed.co.za if you do not want to receive future product or seasonal farm updates.

8. Photo Shoots, Photographs and Children

8.1 Booking information

Information submitted for a photo shoot may be used to check availability, communicate farm access and safety requirements, arrange the session, process payment and retain a reasonable booking record. Photographer details may be shared with the client or relevant farm representative only where necessary for the booking.

8.2 Ownership and use of photographs

A photo shoot booking does not by itself give Hughmari permission to publish identifiable photographs of clients or participants. If the business wants to use photographs or video on its website, social media, advertisements, brochures or other promotional material, it must obtain a clear, separate and recorded media consent. The consent should identify the intended uses and whether names may be used.

8.3 Children and family sessions

For any image of a child, the parent, guardian or other competent person must provide the required consent. The business should avoid publishing the child's full name, precise location, school or other unnecessary identifying details. A competent person may withdraw consent for future use, subject to lawful limitations and material already lawfully published or printed.

8.4 Photographer responsibilities

Independent photographers are responsible for their own POPIA compliance in relation to client images and records. Where a photographer processes personal information on Hughmari's instructions, a written operator agreement must address confidentiality, security, permitted use, incident reporting, return or deletion, and subcontracting.

9. Security Safeguards and Operators

9.1 Minimum safeguards

- Use strong, unique passwords and multi-factor authentication where available for email, website, cloud storage, accounting and social media accounts.
- Limit access to personal information according to role and remove access promptly when a person leaves or no longer needs it.
- Keep computers, phones, applications, website components and security software updated.
- Use device locks, secure backups and appropriate encryption for portable devices and sensitive files.
- Store paper records in locked areas and avoid leaving customer lists, forms or identification information unattended.
- Verify recipient details before emailing, messaging or sharing documents containing personal information.
- Do not use personal information for private purposes or copy it to unapproved apps, devices or cloud accounts.
- Dispose of paper by secure shredding and securely delete electronic records when retention ends.

9.2 Operators and service providers

An operator is a service provider that processes personal information for Hughmari. Examples may include website hosting, email, cloud storage, accounting, payment, marketing, IT support or booking services. The business must conduct reasonable due diligence and use a written agreement requiring the operator to process information only with Hughmari's knowledge or authorisation, maintain confidentiality, implement appropriate safeguards and notify Hughmari immediately of suspected unauthorised access or loss.

9.3 Cross-border processing

Some online services may store or process information outside South Africa. Before using such a service, the business must consider POPIA's requirements for transborder information flows, the protection offered in the destination, contractual safeguards, the nature of the information and whether consent or another lawful basis is required.

10. Security Compromise Response Plan

A security compromise may include loss, unauthorised access, accidental disclosure, ransomware, hacking, theft of a device, an email sent to the wrong recipient, unauthorised publication, or any event affecting the confidentiality, integrity or availability of personal information.

Current reporting position
The Information Regulator states that POPIA does not provide a risk threshold below which a security compromise may be ignored. Once the responsible party is reasonably sure that a compromise has occurred, the Information Officer should report it to the Information Regulator and notify affected data subjects as soon as reasonably possible, subject to lawful delay.

10.1 Immediate response steps

1. Contain the incident: disconnect affected devices where appropriate, revoke compromised access, recall or delete misdirected messages where possible, and preserve evidence.
2. Notify the Information Officer immediately. No staff member may conceal or privately resolve a suspected compromise.
3. Record what happened, when it was discovered, systems and people involved, categories and approximate volume of information, and immediate mitigation taken.
4. Assess whether personal information was accessed, acquired, altered, lost, destroyed or disclosed by an unauthorised person.
5. Notify the Information Regulator through the current prescribed security compromise reporting process as soon as reasonably possible once the business is reasonably sure a compromise occurred.
6. Notify affected data subjects in writing, unless the Regulator or law enforcement directs otherwise. The notice should explain the compromise, possible consequences, measures taken and practical steps the person can take.

7. Investigate root cause, restore secure operations, change controls where necessary and document lessons learned.

10.2 Operator incidents

An operator must notify Hughmari immediately when there are reasonable grounds to believe that personal information processed for Hughmari has been accessed or acquired by an unauthorised person. Hughmari remains responsible for reporting to the Information Regulator and affected data subjects.

11. Data Subject Rights and Request Handling

A data subject may request confirmation of whether the business holds personal information about them and may request access, correction or deletion, object to certain processing, withdraw consent, or complain. Some requests may be limited by law, contractual obligations, legal privilege, the rights of others or applicable retention requirements.

11.1 How to submit a request

Requests may be sent to info@hmlandgoed.co.za or delivered to Farm Frischgewaagd, Trichardt 2300. The business may ask for reasonable proof of identity before releasing or changing information. The current prescribed Information Regulator forms should be used where required.

11.2 Internal process

8. Log the request and acknowledge receipt promptly.
9. Verify identity proportionately and clarify the scope if necessary.
10. Search relevant paper and electronic systems, including email, WhatsApp business records, booking records and accounting files.
11. Assess legal grounds for granting, partially granting or refusing the request.
12. Respond within a reasonable period and explain any lawful refusal or delay.
13. Correct, delete, restrict or annotate the record where appropriate and notify relevant operators or recipients when necessary.
14. Keep a record of the request, decision and action taken.

11.3 Complaints to the Information Regulator

A person who is dissatisfied may lodge a POPIA complaint with the Information Regulator using the current complaint process. The business should first be given a reasonable opportunity to address the concern where appropriate.

12. Retention, Archiving and Secure Destruction

Personal information must not be retained longer than necessary for the purpose for which it was collected, unless retention is required or authorised by law, reasonably required for a lawful purpose related to the business, required by contract, or consented to by the data subject. Records subject to a dispute, investigation, audit or legal hold must not be destroyed until the hold is released.

Record category	Default retention guide	End-of-period action
Customer enquiries that do not become orders	Up to 12 months after the last meaningful contact, unless consent exists for ongoing updates or a dispute requires longer retention.	Delete or anonymise from active systems.
Orders, invoices, receipts and tax-related records	At least five years from the relevant tax return or tax period, and longer where required for an audit, objection, investigation or other legal duty.	Archive securely, then destroy when lawful retention ends.

Record category	Default retention guide	End-of-period action
Photo shoot booking records	Up to three years after the session, or longer while a dispute, unpaid amount or contractual issue remains.	Delete routine booking detail; retain only records needed for legal or accounting purposes.
Photographs used with consent	For the consented purpose and period, subject to withdrawal for future use and any lawful limits relating to material already published or printed.	Remove from future campaigns where consent is withdrawn and reasonably practicable.
Marketing consent and opt-out records	Keep while marketing continues and retain suppression/opt-out evidence as long as necessary to ensure the person is not contacted again.	Retain minimal suppression record rather than deleting the opt-out evidence.
Supplier contracts and payment records	Duration of relationship plus at least five years where relevant to tax, accounting or legal claims.	Securely destroy when no longer required.
Employment and applicant records	According to employment, tax, health and safety, prescription and other applicable legal requirements; unsuccessful application records should generally be limited to a reasonable recruitment period unless consent exists for longer retention.	Securely destroy or anonymise.
Security incident and request logs	At least five years after closure, or longer if required by an investigation, enforcement action, claim or legal hold.	Archive securely and destroy after all related matters are final.

SARS currently states that tax supporting records are generally required for five years, subject to longer retention in specific circumstances such as an outstanding return, audit, investigation, objection or appeal. The business should confirm retention with its accountant and apply any longer period required by another law.

13. Complaints, Training, Monitoring and Review

13.1 Internal complaints

Privacy questions and complaints should be directed to the Information Officer through info@hmlandgoed.co.za or +27 82 666 0893. Complaints must be acknowledged, investigated fairly, documented and resolved as promptly as reasonably possible. The complainant should be informed of the outcome and any corrective action.

13.2 Training and confidentiality

Every person who handles personal information must receive proportionate privacy and security training and must understand the need for confidentiality. Training should cover customer lists, WhatsApp use, email errors, phishing, passwords, paper files, photographs, children's information, marketing consent, requests and incident reporting.

13.3 Monitoring and annual review

The Information Officer should review this manual at least annually and after a material incident, new service, new system, new marketing method, new category of personal information, major supplier change or legal development. The review should verify that the information inventory, operator agreements, security controls, consent records, request logs and retention practices remain accurate and effective.

Annexure A - Personal Information Request Form

Use this internal form to record a request for access, correction, deletion, objection or withdrawal of consent. Where a prescribed Information Regulator form is required, attach or use the latest official form.

Field	Information to complete
Request reference number	
Date received	
Full name of data subject	
Identity verification used	
Contact details	
Relationship with Hughmari	Customer / prospective customer / supplier / employee / photo shoot participant / other
Type of request	Access / correction / deletion / objection / withdrawal of consent / other
Information or record concerned	
Reason or correction requested	
Preferred response method	Email / telephone / collection / other
Decision and legal basis	
Action completed	
Date closed	
Information Officer signature	

_____

Signature of requester

_____

Date

Annexure B - Marketing Consent and Opt-Out Record

Use of prescribed consent form
For unsolicited electronic direct marketing, use the latest prescribed Form 4 and guidance published by the Information Regulator. This annexure is an internal record and does not replace a prescribed form where the law requires it.

Field	Information to complete
Full name	
Telephone / WhatsApp number	
Email address	
Products or services covered	Pomegranate products / photo shoot availability / seasonal farm news / other
Preferred method	WhatsApp / SMS / email / telephone / other
Consent requested on	
Consent granted?	Yes / No
How consent was recorded	Signed form / online form / written message / other
Consent evidence location	
Opt-out or objection date	
Suppression list updated by	

_____
Data subject signature (where applicable)

_____
Date

Annexure C - Photograph and Media Consent Form

This consent is separate from the booking of a photo shoot. Refusing marketing consent must not prevent a person from booking or participating in a session unless publication is genuinely necessary for the specific agreed service.

Field	Information to complete
Client / participant full name	
Photo shoot date	
Photographer	
Description of images or footage	
Permitted uses	Website / Facebook / Instagram / printed marketing / advertising / portfolio / other
May the participant be named?	Yes / No. If yes, specify permitted name or wording.
Consent period	Until withdrawn for future use / fixed period ending _____ / campaign only
Special conditions	
Consent for a child	Name of child (if required): _____ Name and capacity of competent person: _____

I understand the stated use and voluntarily consent to the processing and publication described above. I may contact info@hmlandgoed.co.za to withdraw consent for future use, subject to lawful limitations and material already lawfully published, distributed or printed.

_____

Participant / competent person signature

_____

Hughmari representative

_____

Date

Annexure D - Security Incident and Breach Log

Field	Incident details
Incident reference	
Date and time discovered	
Reported by	
Description of incident	
Systems, files or devices affected	
Categories and estimated number of data subjects	
Categories and estimated volume of records	
Containment and mitigation	
Operator or third party involved	
Information Officer notified	Date / time:
Information Regulator notified	Date / method / reference:
Data subjects notified	Date / method / content:
Reason for any delay	
Root cause	
Corrective action and owner	
Closure date and approval	

Approval

By signing below, the authorised representative confirms that this manual has been reviewed, completed for the business's actual operations and adopted as part of Hughmari Landgoed CC's personal information compliance framework.

Hugh Muirhead Robb Becker
Full name

Chief Executive Officer
Designation


Signature

26.06.2026
Date

Reference Sources

Protection of Personal Information Act 4 of 2013: https://www.gov.za/documents/protection-personal-information-act

Information Regulator - POPIA forms and prescribed forms: https://inforegulator.org.za/popia-forms/

Information Regulator - Information Officers and eServices: https://inforegulator.org.za/information-officers/

Guidance Note on Information Officers and Deputy Information Officers: https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf

Guidance Note on Direct Marketing in terms of POPIA: https://inforegulator.org.za/wp-content/uploads/2020/07/GUIDANCE-NOTE-ON-DIRECT-MARKETING-IN-TERMS-OF-THE-PROTECTION-OF-PERSONAL-INFORMATION-ACT-4-OF-2013-POPIA.pdf

Information Regulator - Fact Sheet: Handling of Security Compromises: https://inforegulator.org.za/2025/08/19/fact-sheet-handling-of-security-compromises/

Information Regulator - contact and complaint information: https://inforegulator.org.za/contact-us/

SARS - Record keeping: https://www.sars.gov.za/client-segments/record-keeping/

Information Regulator contact details (current at publication)
Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg | Telephone: 010 023 5200 | Toll free: 0800 017 160 | General enquiries: enquiries@inforegulator.org.za | POPIA complaints: POPIAComplaints@inforegulator.org.za. Confirm current details on the Regulator's website before submitting a complaint or notification.