

1. PURPOSE AND SCOPE

South African Livestock Agents (Pty) Ltd ("SALA"), trading as Georgie's, is a pork processing company based in Camperdown, KZN. We hereby wish to explain how we acquire, use, retain and disclose your personal information, as is required by the Protection of Personal Information Act 4 of 2013 (referred to as "POPIA" or "POPI").

- Use of the words "we", "us", "our" or "the company" will mean SALA, as may be relevant in each case.
- In general, this policy indicates how and why we collect and process personal information.
- Due to the nature of our business, we are necessarily involved in the collection, processing and disclosure of personal information of clients, prospective clients and other persons who interact or attempt to transact with us. Any person whose information we collect is known as a "data subject" in this policy.
- We may collect and process personal information for any legitimate purpose, including (but not limited to) the following: to ensure that we offer sound and professional services; to ensure the good upkeep, development and safeguarding of our business; and to protect and promote our legitimate interests (collectively, the "SALA Purpose").
- In compliance with POPIA, we commit to processing the personal information of data subjects lawfully and in a reasonable manner that does not infringe the privacy of the data subject.
- This policy must be read together with our PAIA Manual, available on our website at www.georgies.co.za, which sets out the procedure for requesting access to records held by us.

2. WHY WE COLLECT PERSONAL INFORMATION

- In general, we will collect and process personal information as necessary for any legitimate purpose related to the SALA Purpose, including (but not limited to):
 - Performance of any services requested of us;
 - Undertaking of any other activities requested of us;
 - Any further purpose ancillary to the performance of such services or activities;
 - Undertaking of know-your-client and related background checks, which may be required by law or which may be industry practice;
 - Recruitment and related activities;
 - Marketing and related activities.
- Although providing personal information is generally voluntary, we reserve the right to decline to transact or deal with any person who fails to provide personal information which we have requested and which we deem necessary, in our sole discretion. This will also apply to situations where consent is withdrawn or where a data subject objects to the processing of personal information.

3. LAWFUL BASIS FOR PROCESSING

- In terms of section 11 of POPIA, we will only process personal information where at least one of the following lawful grounds applies:
 - The data subject consents to the processing;
 - Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

- Processing complies with an obligation imposed by law;
- Processing protects a legitimate interest of the data subject;
- Processing is necessary for the proper performance of a public law duty; or
- Processing is necessary for pursuing the legitimate interests of SALA or a third party to whom the information is supplied.
- We will identify and document the applicable lawful ground for each processing activity we undertake.

4. HOW WE COLLECT PERSONAL INFORMATION

- Personal information is usually collected directly from a data subject or their representatives. We may collect personal information through electronic communications, meetings, telephone calls and in general dealings with data subjects or their representatives.
- We may refer to a data subject's website and any social media and online profiles, to better understand their activities and ethos and to collect personal information from these and other public platforms.
- We may collect personal information about data subjects from third parties where necessary. In this regard, we may run checks on, inter alia, identity, criminal record and credit history.
- We may monitor activity on any of our IT and electronic networks and our website and gather information about who is visiting and using our website and how, in order to fulfil the SALA Purpose. Our website may use cookies and similar tracking technologies to enhance your experience. You may adjust your browser settings to decline cookies, although this may affect certain functionality.

5. SPECIAL / SENSITIVE PERSONAL INFORMATION

- Certain categories of personal information are afforded additional protection under sections 26–33 of POPIA. These include, but are not limited to, information concerning:
 - Religious or philosophical beliefs;
 - Race or ethnic origin;
 - Trade union membership;
 - Political persuasion;
 - Health or sex life;
 - Biometric information; and
 - Criminal behaviour, including alleged offences.
- We will only process special personal information where:
 - We have obtained the data subject's explicit consent; or
 - Processing is required by law; or
 - Processing is necessary for the establishment, exercise, or defence of a right or obligation in law; or
 - Processing is for historical, statistical, or research purposes.
- Given the nature of our operations, we may process criminal record information as part of background screening for employment or service engagement purposes, as permitted under section 33 of POPIA.

6. CHILDREN'S PERSONAL INFORMATION

- We recognise that the personal information of children (persons under the age of 18) requires special protection in terms of sections 34–35 of POPIA.
- We will not process the personal information of a child unless:
 - The processing is carried out with the prior consent of the child's competent person (parent or guardian); or
 - The processing is necessary for the establishment, exercise, or defence of a right or obligation in law; or
 - The processing is for historical, statistical, or research purposes.
- We do not knowingly market to or collect personal information from children without appropriate parental or guardian consent.

7. SAFEGUARDS, STORAGE AND RETENTION

- We may store personal information physically and/or electronically (which may include cloud-based storage).
- Our servers may be located in various locations, and personal information may be stored in any one of them, subject to section 10 (Trans-border Information Flow) below.
- We have engaged Numata Business IT (Pty) Ltd as our authorised IT operator. Numata administers all IT processes on our behalf, including cybersecurity, data backups, and dark web monitoring. A written data processing agreement is in place with Numata in compliance with section 21 of POPIA.
- We will take reasonable and appropriate technical and organisational measures to keep personal information secure against loss, damage, or unauthorised access, including:
 - Cybersecurity controls administered by our IT operator;
 - Regular encrypted data backups;
 - Dark web monitoring to detect any compromise of our data; and
 - Access controls limiting personal information to authorised personnel only.
- We cannot guarantee the absolute security of personal information transmitted over the internet.
- We will retain personal information only for as long as is necessary for the purpose for which it was collected, or as required by law. The following general retention schedule applies:

Category	Retention Period	Legal Basis
Client / supplier records	7 years after end of relationship	Tax Act / Companies Act
Employee records	5 years after termination	BCEA / LRA
Recruitment records (unsuccessful)	12 months after decision	POPIA s.14
Background check records	Duration of engagement + 3 years	POPIA s.14
Marketing consent records	Duration of consent + 3 years	POPIA s.69
CCTV / access logs	30 days (unless subject to dispute)	POPIA s.14
Website / cookie data	12 months	POPIA s.14
Financial records	7 years	SARS / Companies Act

8. EMPLOYEES AND THIRD PARTIES

- To carry out the SALA Purpose, the company's owners, managers, employees and consultants will need to review, consider, verify and discuss the personal information collected by it.
- To carry out the SALA Purpose, we may transfer or disclose personal information to third party contractors, subcontractors, and/or their subsidiaries and affiliates.
- Examples of third party contractors we use include:
 - Numata Business IT (Pty) Ltd — IT infrastructure, cybersecurity, backups, and dark web monitoring;
 - Providers of website management, cloud storage and related services;
 - Professional advisers (legal, audit, and compliance).
- We will ensure that a written data processing agreement (as contemplated in section 21 of POPIA) is in place with any third party operator that processes personal information on our behalf.
- Where required by law, some or all of the personal information collected by us may be disclosed to any governmental authority or regulatory body.
- We may also disclose your personal information to third parties where necessary to carry out the services or activities requested of us, or to protect our legitimate interests.

9. TRANS-BORDER INFORMATION FLOW

- If we collect or process your personal information, your personal information may be transferred to and stored outside South Africa or the country where you are located. This may include countries that do not have laws that provide specific protection for personal information.
- In general, the company will not transfer personal information to a party in a foreign country, unless:
 - a. the data subject consents to the transfer, or
 - b. the transfer is necessary for us to perform in terms of a contract or for the implementation of pre-contractual measures taken in response to a request from the data subject; or
 - c. the foreign country has a law that provides adequate protection; or
 - d. there is an agreement between the company and the relevant foreign party that provides adequate protection; or
 - e. there are binding corporate rules that provide adequate protection.

10. DATA BREACH NOTIFICATION

- In the event that we reasonably believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, we will, in compliance with section 22 of POPIA:
 - Notify the Information Regulator as soon as reasonably possible after becoming aware of the compromise; and
 - Notify the affected data subject(s), unless the identity of the data subject(s) cannot be established.
- Such notification will be communicated in writing and will include:
 - A description of the possible consequences of the security compromise;
 - A description of the measures being taken or to be taken to address the security compromise;
 - A recommendation regarding the steps the data subject should take to mitigate the effects; and

- The identity of the unauthorised person who accessed the information, if known.
- Our IT operator, Numata Business IT (Pty) Ltd, assists us with dark web monitoring and cybersecurity incident response to detect and contain potential breaches as early as possible.

11. DIRECT MARKETING

- We may only use personal information of a data subject for the purposes of direct marketing if:
 - We have obtained the data subject's prior consent (opt-in); or
 - The data subject is an existing customer and the marketing relates to similar products or services, and the data subject has been given a reasonable opportunity to opt out on each communication.
- Consent for direct marketing may be obtained in writing, electronically, via SMS, WhatsApp, or by means of a recorded telephone call, as permitted under POPIA and its Regulations.
- Every direct marketing communication will include a clear and easy mechanism for the data subject to opt out or unsubscribe. We will honour all opt-out requests promptly.
- We will keep a record of all marketing consents obtained and the means by which consent was recorded.

12. AUTOMATED DECISION-MAKING

- In terms of section 71 of POPIA, a data subject has the right not to be subject to a decision which results in legal consequences for them, or which affects them to a substantial degree, and which is based solely on the automated processing of personal information.
- Where we make use of any automated processing that results in such decisions, data subjects will be informed accordingly and will have the right to request that such decision be reconsidered by a person.

13. DATA SUBJECT RIGHTS

- We will take reasonable and appropriate measures to accurately record a data subject's personal information as provided by them or their representatives and make reasonable efforts to ensure that personal information is complete, accurate and not misleading.
- Data subjects have the right to access their personal information and the right to request the correction, reduction or deletion thereof, subject to reasonable qualifications.
- Any such request must be in writing and submitted to the Information Officer. We will respond to all requests within 30 (thirty) business days of receipt, unless an extension is agreed or required by law.
- Each data subject has the right to:
 - Withdraw any of the consents given in relation to the processing of their personal information (however, we may continue to process the personal information to the extent necessary to implement a contract with the data subject, or to protect the legitimate interests of the data subject, or to protect our legitimate interest, or to comply with any legal obligation);
 - Ask us to reveal what personal information we have relating to the data subject and who has had access to that information (in which case we will respond within 30 business days);
 - Ask us to correct or delete any of their personal information which is inaccurate, irrelevant, out of date, incomplete or misleading (in which case we will respond by altering our records, or substantiating our records, as appropriate, within 30 business days);

- Ask us to destroy or delete any of their personal information if it is no longer lawful for us to retain it (in which case we will respond within 30 business days, allowing time for us to seek legal advice if necessary);
- Object to us processing any of their personal information where the processing is:
 - a. not covered by consent;
 - b. not necessary for carrying out a contract between us and the data subject;
 - c. not necessary to discharge a legal obligation or protect our legitimate interests, and provided that the data subject has reasonable grounds for objection (in which case we will cease processing the personal information);
- Object to the processing of their personal information to prevent any direct marketing by us (in which case we must cease processing the personal information for this purpose);
- Lodge a complaint to the Information Regulator at:

JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
PO Box 31533, Braamfontein, Johannesburg, 2017
Tel: 010 023 5207 | Email: complaints.IR@justice.gov.za / inforeg@justice.gov.za

14. INFORMATION OFFICER

- SALA has registered its Information Officer and Deputy Information Officer with the Information Regulator as required by section 55 of POPIA and Regulation 3. Registration details are as follows:
 - Information Regulator Registration Number: 2026-007306
 - Registration Date: 13 April 2026
- Please direct all queries relating to this policy or the processing of your personal information to our Information Officer:

Name and Surname	Role	Contact / Email
Ryan Dean Bruwer	Information Officer	+27 (0)31 785 2179 ryan@salapork.co.za
Ryan David Thompson	Deputy Information Officer	Available on request

15. ACCEPTANCE

The data subject consents to the collection, processing, disclosure, storage and general treatment of personal information described in this privacy policy, and as may be necessary to fulfil the SALA Purpose, by:

- agreeing to our terms of engagement; or
- agreeing to our standard terms and conditions (STCs); or
- using our services, transacting, or otherwise dealing with us after being advised of our terms of engagement or STCs or this privacy policy; or
- by providing us, or permitting us to be provided with, their personal information in order for us to carry out any service or legitimate activity.

16. REVISION HISTORY

We may update this privacy policy at any time by publishing an updated version on our website. When we make material changes to this policy, we will notify data subjects by email or prominent notice on our website, and amend the revision date. The updated policy will apply from the effective date.

Version	Revision Date	Effective Date
SALAv1	June 2021	01 July 2021
SALAv2	April 2026	01 April 2026