

Confidential



Registered credit provider: Reg. Number NCRCP18

LAND AND AGRICULTURAL DEVELOPMENT BANK EMPLOYEE PRIVACY NOTICE



I BACKGROUND AND PURPOSE OF THIS NOTICE

- 1.1. The Land and Agricultural Development Bank of South Africa ("Land Bank" or "the Bank ") has developed this Employee Privacy Notice ("Notice") to explain how it collects, uses, processes, stores, and protects Personal Information relating to employees and prospective employees, in accordance with the requirements of the Protection of Personal Information Act, No. 4 of 2013 ("POPIA").
- 1.2. The Bank undertakes to process Personal Information in compliance with POPIA and all other applicable laws, and to implement appropriate measures to safeguard the confidentiality, integrity, and availability of Personal Information.

2 SCOPE

- 2.1. This Notice applies to the personal information of all employees and prospective employees of the Bank.
- 2.2. This includes individuals whose personal information is processed during recruitment, appointment, employment, secondment, and termination processes.
- 2.3. This Notice applies to personal information collected in any form, whether provided directly by the employee or prospective employee, obtained from third parties, or generated during the course of employment.

3 DEFINITION OF EMPLOYEES' PERSONAL INFORMATION

Personal information has the meaning assigned to it in POPIA and includes information relating to an identifiable, living natural person and, where applicable, an identifiable existing juristic person.

Personal information, processed by the Bank regarding employees, includes but is not limited to the following types of information:

Term	Description
Personal details	Name, surname, gender and sex, address, contact details, emergency contact details and next of kin information, birth certificate number, identity number, passport number, age, marital status, language(s) spoken and financial history.

Basic work details	Work contact details (such as corporate email address and telephone number), unique employee numbers, photographs, employment start and end dates and places of work.
Professional qualifications and regulatory information	Qualifications, degrees, and certifications.
Recruitment and selection information	Personal information contained in CVs, including employment history, academic records, employment applications, reference letters, interview records, interview notes, assessments, tests, vetting, and verification documents.
Credit records and financial interests	Credit records, financial interests and outside business interests or conflict of interest declarations.
Remuneration and benefits information	Details of compensation and benefits, bank account details, employment grades, tax information, expense claims, travel, and claims.
Leave information	Absence records, including annual leave, maternity leave, and family-related leave records.
Disciplinary and grievance information	Personal information contained in records of allegations, investigations, meeting records, and outcomes.
Performance management information	Colleague and manager feedback, appraisals, output from talent programmes, formal and informal performance management processes.
Training and development information	Data relating to training and development needs or training received.
Monitoring information	Where permitted by law, identifiable images or video images contained in CCTV footage, system and building login and access records, keystrokes, internet activity, location data, printing records, call recordings, data caught by IT security programs, filters, and security monitoring software.

Termination or end of employment information	Dates and reasons for leaving employment, termination arrangements and payments, exit interviews and references.
Information of dependants	Personal information about an employee's dependent family members (including nominated beneficiaries and next of kin) such as their names, surnames, and dates of birth, contact information).
Special Personal Information	<p>There are special categories of an employee's personal information which Land Bank will only process where a heightened set of requirements are met. Special categories of personal information include information concerning:</p> <ul style="list-style-type: none"> • religion or philosophical beliefs; • race and ethnic origin; • trade union membership; • health and sex life; • biometric information; and • certain information concerning criminal behaviour or criminal offences.

4 WHEN AND WHY LAND BANK COLLECTS AND PROCESSES PERSONAL INFORMATION

Personal information will be processed by Land Bank in the normal course of business of managing employees for various purposes, including but not limited to the following:

- 4.1 assess suitability for employment, including verifying qualifications, calling references, and conducting psychometric and other assessments;
- 4.2 obtain required banking information to process an employee's remuneration, benefits, and incentives;
- 4.3 facilitate the admission and administration of employees and their beneficiaries to retirement benefits, pension, or provident fund arrangements;
- 4.4 facilitate the admission and administration of employee and dependants to medical aid providers, provide a subsidy where applicable and provide the relevant administration (may include the personal information of an employee's dependants);

- 4.5 keep proof of medical aid membership in cases where an employee elects to be a dependant on another person's scheme, other than the Bank's medical aid providers, to comply with conditions of employment;
- 4.6 comply with the group's anti-money laundering and terrorist financing, and fraud and corruption detection obligations, as well as risk management processes implemented by the bank including conducting screening such as politically exposed persons (also known as PEP), Southern African Fraud Prevention Service (SAFPS);
- 4.7 comply with all applicable laws authorising or requiring such processing, including (but not limited to) the Basic Conditions of Employment Act 75 of 1997, the Labour Relations Act 66 of 1995, the Employment Equity Act 55 of 1998, the Occupational Health and Safety Act 85 of 1993, the Financial Intelligence Centre Act 38 of 2001, the Prevention and Combating of Corrupt Activities Act 12 of 2004, the Companies Act 71 of 2008 and the Skills Development Act 97 of 1998, including all relevant regulations;
- 4.8 conduct any specific obligations and duties of the bank in the field of employment legislation;
- 4.9 realise objectives laid down by or by virtue of tax or other applicable legislation;
- 4.10 properly assess performance under an employment contract;
- 4.11 undertake management activities, such as succession planning, talent management, training, work planning, managing tasks, assessing the performance of the employees, and controlling security and access to facilities;
- 4.12 monitor, record or report employees' access to buildings for safety and security purposes;
- 4.13 investigate and conclude on the outcome of matters that were referred to the independent ethics line (whistleblowing line), including conduct of employees;
- 4.14 share employees' children's details, e.g. pension benefits on the death of a parent or if the parent signs up the child(ren) and
- 4.15 share close relatives' details, for example emergency contact persons.

5 PURPOSE OF THE PROCESSING OF SPECIAL PERSONAL INFORMATION

The Bank may process special personal information for various reasons and, where required, with the employee's necessary consent.

5.1 Race and ethnic information may be collected and processed to monitor employment equity and diversity goals or comply with regulatory reporting and employment equity obligations.

5.2 Health information, medical and health related information

- In the event of a work-related injury, may process health information to comply with its obligations under the Occupational Health and Safety Act 85 of 1993, or to process claims under the Compensation for Occupational Injuries and Diseases Act, 130 of 1993.
- The Bank may need to collect personal information for purposes of absence records, such as medical forms or doctor's notes. Information regarding an employee's disability may be required to provide reasonable accommodation.

5.3 Biometric information

The Bank may collect biometric information, such as a fingerprint, to identify and verify identity, and provide access to secure facilities.

5.4 Criminal behaviour and offences

The Bank may collect and process information regarding criminal behaviour and/or offences for employee background screening activities, including screening on national and international databases for fraud, dishonest conduct, and/or employment dismissal due to unlawful action.

Land Bank will not retain or process special personal information unless one of the lawful reasons applies. For example (where the law requires consent) a specific consent relevant to the processing of biometric personal information will be requested by the bank)

6 LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION

The Bank will process an employee's personal information pursuant to a lawful justification, including:

- 6.1. employee or prospective employee has provided consent;
- 6.2. performance of the employment contract to which the employee is party or to take steps prior to entering the employment contract;
- 6.3. compliance with legal obligations that are imposed by legislation or regulations or otherwise as may be applicable;
- 6.4. protection of a legitimate interest of the Bank, employee, or a third party;
- 6.5. processing is necessary for purposes of security, risk management, governance, and compliance and
- 6.6. withdrawal of consent will not affect processing activities that are conducted on another lawful basis permitted under POPIA, including compliance with legal obligations or performance of the employment relationship.

7 SOURCES OF PERSONAL INFORMATION

- 7.1 Personal information will be primarily collected directly from the employee, either during the employee's application for employment or engagement, the onboarding process, or on an ad hoc basis during employment or the relationship.
- 7.2 During the recruitment process, the Bank may request references from third parties and conduct screening and vetting processes using third-party sources. The Bank will conduct such screening and vetting processes only to the extent permitted, contemplated, or required by law.
- 7.3 The Bank may also receive personal information about an employee from:
- 7.3.1 third parties, for example clients, tax authorities, benefit providers, and regulatory bodies to the extent permitted, contemplated, or required by law;
 - 7.3.2 security systems monitoring, including access control systems, CCTV, telephone recordings, email systems, and internet usage logs. Monitoring activities will be conducted in a lawful, reasonable, and proportionate manner and only to the extent necessary for legitimate business, security, operational, compliance or legal purposes;
 - 7.3.3 technology and digital platforms, including systems used to manage employee credentials, access rights, and workplace tools.
- 7.4 The Bank will take reasonable steps to ensure that personal information collected from third parties is processed lawfully and that employees are made aware of such collection where required under applicable law.

8 SHARING OF PERSONAL INFORMATION

- 8.1. The Bank may share personal information where such sharing is lawful, necessary, and consistent with the purposes set out in this Notice.
- 8.2. The Bank may share personal information with third parties under the following circumstances:
- 8.2.1 service providers - we may share your personal information with our service providers that perform business operations for us, for example, we subcontract our criminal background checks to third party service providers;
 - 8.2.2 any law enforcement agency, court, regulator, government authority, or other third party - we may share your personal information with these parties where we believe this is necessary to comply with a legal or regulatory obligation or otherwise to protect our rights or the rights of any third party; or

- 8.2.3 any third party – we may share your personal information with any third party where we believe we are compelled by applicable law or regulation, if we find it necessary to exercise, establish or defend our legal rights, to protect the Bank's rights or property, to protect the public from harm or illegal activities, or to respond to an emergency which we believe, in good faith requires us to disclose personal information to prevent harm.

We will only share your personal information in accordance with requirements as set out in POPIA.

9 SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

- 9.1 All personal information processed by the Bank is confidential and treated as such and the Bank will take reasonable, appropriate technical and organisational measures to keep personal information secure, in accordance with its information security policies and procedures and any applicable legislation.
- 9.2 Any third party who processes your personal information on our instruction is subject to the terms and conditions of an operator agreement. We evaluate these measures on a regular basis to ensure the security of the processing.
- 9.3 The Bank regularly reviews and updates its security measures to ensure ongoing effectiveness and alignment with legal and regulatory requirements.

10 RETENTION OF PERSONAL INFORMATION

- 10.1. The Bank may retain personal information to:
- 10.1.1. comply with applicable legal, regulatory, and statutory requirements and
 - 10.1.2. fulfil obligations arising from the employment relationship.
- 10.2. where retention is required to protect the legitimate interests of the Bank.
- 10.3. Furthermore, as a government entity, we are required to adhere to the provisions of the National Archives and Records Service of South Africa Act No. 43 of 1996, to manage and preserve government records.
- 10.4. The Bank will take reasonable steps to delete, destroy, or de-identify personal information once it is no longer required for lawful purposes.
- 10.5. Where the Bank is unable to delete personal information due to technical or legal constraints, it will take appropriate measures to restrict further processing of such information.

11 PERSONAL INFORMATION QUALITY MANAGEMENT

- 11.1. The Bank will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate and not misleading, and is updated where necessary.
- 11.2. People and Culture functions have provided the self-service portal through which employees are required to update their personal information if it changes. Each employee is responsible for using these channels to update their personal information, when necessary.
- 11.3. For updates to personal information that are not made possible through the self-service portal, employees must address their request to the responsible human capital department.

12 CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

- 12.1 The Bank may transfer personal information to recipients located outside of the Republic of South Africa where this is necessary for the purposes set out in this Notice.
- 12.2 Where personal information is transferred across borders, the Bank will ensure that such transfers are conducted in accordance with POPIA.
- 12.3 The Bank will implement appropriate safeguards to protect the confidentiality, integrity, and security of personal information when it is transferred outside of South Africa.

13 Employees' privacy rights

13.1 Access to information

An employee has the right to access the personal information which relates to them. Where an employee wishes to request personal information, which personal information is needed to protect a right of the employee, a request must be addressed in accordance with the people and culture procedures. Certain personal information relevant to the employee may be accessed through self-service portal.

13.2 Right to correction of personal information

An employee has the right to correct inaccurate personal information which relates to them. The employee can update and correct certain types of personal information stored on the human capital platform using a self-service channel. For instructions on how to do so, the employee should contact the responsible people and culture business partner.

13.3 Right to deletion

An employee is entitled to require the destruction/deletion of their personal information which is by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or unlawfully obtained and
- retained beyond a reasonable period after the end of the employment contract between the parties.

13.4 Right to withdraw consent

Where an employee has provided their consent for their personal information to be processed, the employee has the right to withdraw consent at any time, without affecting the lawfulness of processing based on the consent before its withdrawal.

13.5 Right to object

Employees have the right to object, on reasonable grounds, to the processing of their personal information where the processing is carried out to protect Land Bank's legitimate interest, the legitimate interest of a third party with whom the personal information was shared, or the employee's legitimate interest, unless the law provides for such processing.

13.6 Right to lodge a complaint

Employees have the right to lodge a complaint with the Information Regulator if they believe that their personal information has been processed unlawfully or unfairly. The Information Regulator's details can be found on the Information Regulator's website at <https://inforegulator.org.za/>.

13.7 Employees are encouraged to contact the Bank in the first instance to address any concerns relating to the processing of their Personal Information.

13.8 Requests to exercise any of the above rights must be submitted in writing in accordance with the procedures set out in the Bank's PAIA Manual which may be accessed on the Bank's intranet or website.

I4 CONTACT DETAILS

14.1. Information Officer Contact Details (Land Bank)

Information Officer: Chief Executive Officer

Physical Address:

272 Lenchen Avenue, Lakefield Office Park,
Building A, First Floor,
Die Hoewes, Centurion

Postal Address:

P.O. Box 375, Tshwane, 0001

Telephone: 012 686 0591

Fax: 012 686 0588

Website: <https://landbank.co.za>

Email: PAIA@landbank.co.za

14.2. Information Regulator Contact Details

Physical Address:

Woodmead North Office Park,
54 Maxwell Drive,
Woodmead, Johannesburg, 2191

Telephone: +27 (0)10 023 5200

Website: <https://inforegulator.org.za>

Complaints email: POPIAComplaints@inforegulator.org.za

General enquiries email: enquiries@inforegulator.org.za

I5 OTHER POLICIES

This Notice must be read in conjunction with the Bank's other policies on data protection and privacy.