

DATA PROTECTION POLICY

1. POLICY STATEMENT, PURPOSE AND OBJECTIVES

1.1 Overview

OI Pejeta Ranching Limited and OI Pejeta Conservancy Limited hereinafter individually and jointly referred to as (“the Conservancy”) has developed this Data Protection Policy (“Policy”) in recognition of its statutory obligation outlined under the Data Protection Act, 2019 and its enabling regulations.

1.2 Purpose

This Data Protection Policy (“the policy”) has been established to provide guidelines and framework on how the Conservancy shall process personal and sensitive data of its employees, suppliers, stakeholders and other third parties towards compliance with the provision of the Data Protection Act, 2019 and its enabling regulations. This Policy:

- 1.2.1** Establishes the required framework for privacy and protection of data held by the Conservancy while proactively responding to the legal and regulatory compliance obligations stipulated under the Act.
- 1.2.2** Ensures effective protection and management of Data by identifying, assessing, monitoring and mitigating privacy risks in any activities involving the collection, retention, use, disclosure and disposal of Data by the Conservancy.
- 1.2.3** Ensures the Conservancy has internal controls and mechanisms in place that adequately mitigate any risks of data breaches.
- 1.2.4** Creates and embed a culture of compliance to data protection and privacy across the Conservancy.
- 1.2.5** Reduces the risks financial losses to the Conservancy arising from penalties that may be imposed as a result of Personal Data Breaches and non-compliance with applicable laws.

1.3 Scope

This Policy shall apply to all directors, employees, consultants, interns, or any other stakeholder employed by the Conservancy and who processes personal data. It covers all personal data collected, stored, accessed, or otherwise processed by the organization in the course of its operations, whether in electronic or physical form.

1.4 Abbreviations & Definitions

Anonymization	Means the removal of personal identifiers from personal data so that the Data Subject is no longer identifiable.
Consent	Means any manifestation of express, unequivocal, free, specific, and informed indication of the Data Subject’s wishes by a statement or by a clear affirmative action, signifying their agreement to the processing of data relating to the Data Subject.
Data Controller	Means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of Personal Data.
Data Processor	Means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
Data Subject	Means an identified or identifiable natural person who is the subject of Personal Data.
Encryption	Means the process of converting the content of any readable data using technical means into coded form.

Certificate of Registration	Means a valid Certificate issued by the Office of the Data Commissioner upon registration as a Data Controller and/or Data Processor.
Complaints Register	Means a register maintained by the Data Protection Officer outlining all complaints received by Data Subjects, investigations and details of the outcome of investigations and how their complaints have been addressed by the Conservancy.
Compliance Reports:	Means information and data showing the Conservancy's status of compliance with all applicable legal and regulatory requirements on data protection including any Personal Data Breaches and complaints from Data Subjects.
Personal Data	Means any information relating to an identified or identifiable natural person.
Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed by the Conservancy.
Pseudonymization	Means the processing of data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
Regulator	Means the Office of the Data Commissioner established under the Act to regulate compliance with data protection laws and principles by Data Controllers and Data Processors and take enforcement actions in the case of non-compliance.
Sensitive Personal Data	Means personal data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse(s), sex or the sexual orientation of the Data Subject.
Staff	Means employees of The Conservancy.
Third Party	Means natural or legal person, public authority, agency or other body, other than the Data Subject, Data Controller or Data Processor who, under the direct authority of the Data Controller or Data Processor, are authorized to process Personal Data.
Training Program	Means a set of activities intended to create awareness and ensure adherence to the Data Protection Act, 2019 across all cadres of employees.

2. RATIONALE

In the digital era, data is a critical resource that drives economic growth and owing to the rising amount of Personal and Sensitive Data being processed, various data protection laws and regulations have been put in place with the aim of ensuring security and privacy of such data. In this regard, the Conservancy is required to comply with various laws and regulations including but not limited to;

2.1 The Constitution of Kenya, 2010

2.2 The Data Protection Act, 2019

2.3 The Data Protection (General) Regulations, 2021

2.4 The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021

- 2.5** The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021
- 2.6** Any other Regulatory requirements including relevant circulars, guidelines, codes and directives issued by Regulators and other forms of established codes and practices.

3. PRINCIPLES OF DATA PROTECTION

In processing of Personal Data, the Conservancy will comply with the following guiding principles:

- 3.1** Personal data shall be processed in accordance with the right to privacy of the Data Subject.
- 3.2** Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. The Conservancy will inform individuals about why their data is needed, how it will be used, and who it may be shared with, the safeguards adopted to secure the data their rights over the data and the consequences (if any) of failing to provide the data. This will be done through clear notices, and explanations will be provided where sensitive personal or family matters are involved.
- 3.3** The processing of Personal Data shall happen in a lawful way and shall have a legal and legitimate basis. Data will only be collected and used when there is a valid reason under the law, such as where the individual has given consent, or the data is needed to fulfil a contract, comply with a legal obligation, or protect vital interests. The legal basis for each processing activity must be documented in the privacy notice shared with the Data Subject. For more information on the lawful basis for processing personal data, refer to Clause 5 of this Policy.
- 3.4** Personal Data collected by the Conservancy shall only be used for the purpose that was defined before the data was collected and shall not further be processed or used in a manner that is incompatible or inconsistent with those purposes.
- 3.5** Personal Data collected shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the data will be processed. This means that the Conservancy only collects and uses the minimum amount of data necessary for a specific purpose.
- 3.6** Personal data shall not be kept for longer periods than is necessary to achieve the purpose for which the data was collected and processed. Personal Data kept by the Conservancy shall be retained guided by its internal Policies.
- 3.7** Personal data maintained by the Conservancy shall be accurate, complete, and as practically possible up to date. The Conservancy will take suitable steps to ensure that data maintained by it is updated.
- 3.8** The Conservancy shall establish suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction of Data.
- 3.9** The Conservancy shall not transfer or disclose Personal Data to a Third Party without the Data Subject's Consent and unless there is adequate proof of adequate data protection safeguards by the Third Party.
- 3.10** The processing of personal data for a child shall be done only with the Consent of the child's parent or guardian.

4. RIGHTS OF A DATA SUBJECT

- 4.1** In processing Personal Data, the Conservancy shall be cognizant of the following rights of Data Subjects:
 - 4.1.1** Right to be informed of the use to which their personal data is to be put.
 - 4.1.2** Right to access of their personal data held by the Conservancy.
 - 4.1.3** Right to object to the processing of all or part of their personal data.
 - 4.1.4** Right to rectification if the information held is inaccurate, false, misleading or is incomplete or requires to be updated.
 - 4.1.5** Right to complain (as would be appropriate to the Data Controller, Data Processor or Regulator)
 - 4.1.6** The right to object the processing of their data for Direct Marketing purposes.
 - 4.1.7** The right to be forgotten/ the right to erasure.

- 4.1.8** Right to appropriate security safeguards where personal data is being archived for various purposes.
- 4.1.9** The right to appropriate security safeguards in cross border transfer of personal data.
- 4.2** All staff handling personal data will be trained on how to recognize and appropriately escalate or respond to data requests received from Data Subjects.
- 4.3** Where a data subject is dissatisfied with the handling of their data rights, the Conservancy will provide a clear internal complaint handling process.

5. EXERCISING DATA SUBJECT RIGHTS

- 5.1** In processing Personal Data, the Conservancy shall be cognizant of the following rights of Data Subjects:
- 5.2** The Conservancy shall provide all Data Subjects with accessible and transparent procedures to exercise their rights under the Data Protection Act, 2019.
- 5.3** To protect personal data and individual privacy, the Conservancy will verify the identity of the requesting individual before granting access or making changes.
- 5.4** Where a request is made on behalf of another person (e.g. a parent on behalf of a child), appropriate proof of authority will be required.
- 5.5** The Conservancy will respond to requests related to data subjects within the time frames required by law.
- 5.6** The exercise of data subject rights shall be free of charge.
- 5.7** All requests and the actions taken shall be logged and retained as part of the Conservancy's data protection records.
- 5.8** Data Subjects may contact the Conservancy's designated Data Protection Officer (DPO) or responsible officer for assistance with understanding or exercising their rights.

6. LEGAL BASIS FOR PROCESSING DATA

- 6.1** Processing of personal and sensitive personal data by the Conservancy shall be based on at least one of the following lawful basis:
 - 6.1.1** Consent from the data subject
 - 6.1.2** Parental or guardian consent in case of children's data.
 - 6.1.3** Performance of a contract
 - 6.1.4** Legal obligation
 - 6.1.5** Vital interest of the data subject
 - 6.1.6** Legitimate interest of the Conservancy or a third party (balanced against the rights of the data subject)
 - 6.1.7** Public interest or performance of a statutory duty
 - 6.1.8** Historical, artistic, literature or research purposes
- 6.2** The Conservancy will include the legal basis for processing in all relevant privacy notices provided to Data Subjects.

7. PERSONAL DATA COLLECTION

- 7.1** The Conservancy shall collect personal data in a manner that is lawful, fair, and transparent.
- 7.2** Data shall be collected either directly from the Data Subject or indirectly through permitted means, in accordance with the Data Protection Act, 2019.
- 7.3** The Conservancy will prioritise the collection of personal data from the data subject whenever possible which may include without limitation to collecting information directly from visitors, community members, staff, volunteers, or contractors through forms, interviews, or registration systems.
- 7.4** Where direct collection is not possible, the Conservancy may collect personal data from third-party sources or public records.

8. DATA PROTECTION OFFICER

The Conservancy hereby designates the Legal Coordinator/Counsel as its Data Protection Officer ("the DPO") The DPO shall be responsible for:

- 8.1** Ensuring that the Conservancy processes personal data of its staff, customers, service providers or any other individuals in compliance with the Act.
- 8.2** Advising the Conservancy and employees on data processing requirements and facilitate capacity building for staff involved in data processing operations.
- 8.3** Applying for registration of the Conservancy as a Data Controller and Data Processor and thirty days before the expiry of the Certificate of Registration, apply for renewal of the Certificate of Registration.
- 8.4** Monitoring new and on-going data protection risks of the Conservancy.
- 8.5** Conducting and advise the Conservancy on Data Protection Impact Assessment with a view of mapping out all the data processed and held by the Conservancy while assessing the impact and risks of the processing activities.
- 8.6** Conducting continuous trainings and awareness sessions across the Conservancy on data privacy requirements and obligations of the Conservancy.
- 8.7** Supporting data incident management, investigations and Data Breach notifications to the Office of the Data Commissioner.
- 8.8** Receiving, investigating and addressing complaints from Data Subjects regarding their Data held by the Conservancy and maintaining a Complaints Register.
- 8.9** Providing Compliance reports and status updates on the data protection and privacy obligations of the Conservancy to the Senior Leadership Team.
- 8.10** Liaise and cooperate with the Office of the Data Commissioner and any authority on matters relating to data protection while ensuring that all the risks related to data protection are captured in the register and addressed appropriately.
- 8.11** Make regular compliance reports on data protection to the Office of the Data Commissioner.

9. DEPARTMENTAL DATA PROTECTION LEADS

- 9.1** The DPO retains ultimate responsibility for ensuring that a culture of compliance and data privacy is engendered across the Conservancy and that the data held by the Conservancy is safeguarded as required under the Act.
- 9.2** Each department shall appoint a Data Protection Lead (DPL) to:
 - 9.2.1** Coordinate data privacy efforts at the department level;
 - 9.2.2** Report concerns to the DPO;
 - 9.2.3** Implement and monitor department-specific controls.

10. DATA SECURITY

- 10.1** The Conservancy shall implement organizational, physical, and technical and security measures to enhance its data security and minimize any incidences of breach. These measures shall include without limitation to:
 - 10.1.1** Firewalls, passwords, antivirus, encryption, and secure authentication.
 - 10.1.2** Access control measures to restrict access to personal data to those who require it for their work
 - 10.1.3** Physical security measures such as locked cabinets and limited access to physical storage rooms
 - 10.1.4** Ensuring that personal data shared with personal data is protected by using secure transfer methods and entering into data processing or data sharing agreements with third parties who process personal data on behalf of the Conservancy.
 - 10.1.5** Implementing processes and mechanisms to ensure secure disposal of records;
 - 10.1.6** Conducting Regular security assessments and audits.

11. DATA PROTECTION IMPACT ASSESSMENTS

- 11.1** The Conservancy shall conduct Data Protection Impact Assessments (DPIAs) to identify and minimise the risks to personal data arising from processing activities that are likely to result in a high risk to the rights and freedoms of Data Subjects.
- 11.2** The Conservancy may carry out a DPIA in the following situations:
 - 11.2.1** Introduction of new systems or technologies that involve personal data (e.g. new databases, surveillance tools, biometric systems).
 - 11.2.2** Large-scale processing of sensitive or special category data (e.g. health, children's data).
 - 11.2.3** Systematic monitoring or profiling of individuals.
 - 11.2.4** Any other processing activity likely to result in a high risk to Data Subjects, as determined by the Data Protection Officer (DPO) or applicable law.
- 11.3** When conducting a DPIA, the Conservancy shall:
 - 11.3.1** Describe the nature, scope, context, and purpose of the processing.
 - 11.3.2** Assess the necessity and proportionality of the processing in relation to its purpose.
 - 11.3.3** Identify and assess the potential risks to the rights and freedoms of Data Subjects.
 - 11.3.4** Propose measures to mitigate identified risks and demonstrate compliance with data protection principles.
 - 11.3.5** Consult with relevant stakeholders, including the DPO and, where required, the Office of the Data Protection Commissioner (ODPC).
- 11.4** The responsibility for initiating and overseeing a DPIA shall be jointly conducted with the DPO in liaison with the department proposing a new or change in data processing activity.
- 11.5** Where risks cannot be mitigated to an acceptable level, the DPO shall advise whether to proceed and, where necessary, consult with the ODPC before implementation.
- 11.6** All DPIAs must be documented and retained as part of the Conservancy's compliance records.
- 11.7** DPIAs shall be reviewed periodically, especially when changes occur to the processing activity, technology, or legal requirements.

12. DATA BREACH RESPONSE PLAN

- 12.1** The Conservancy is committed to responding promptly and effectively to any actual or suspected personal data breach to minimize harm to individuals and to ensure compliance with the Data Protection Act, 2019.
- 12.2** All staff, contractors, and third parties handling personal data on behalf of the Conservancy must report any actual or suspected data breach immediately to the designated Data Protection Officer (DPO).
- 12.3** Where the breach poses a risk to the rights and freedoms of individuals, the Conservancy shall notify the Office of the Data Protection Commissioner (ODPC) without undue delay, and no later than 72 hours after becoming aware of the breach.
- 12.4** If a data breach is likely to result in high risk to the rights and freedoms of the data subjects, the conservancy will notify the affected individuals without undue delay.
- 12.5** All personal data breaches, whether or not they are reportable, shall be documented in the Conservancy's personal data breach register.

13. DATA RETENTION AND DISPOSAL

- 13.1** Personal data shall be retained only for as long as necessary for the purposes for which it was collected or as required under applicable law, after which it shall be securely destroyed.

- 13.2** The Conservancy shall define and apply specific retention periods for different categories of personal data, based on:
- 13.2.1** The purpose for which the data was collected
 - 13.2.2** Legal or regulatory requirements
 - 13.2.3** Operational needs
 - 13.2.4** The rights and expectations of the Data Subject
- 13.3** Where feasible, personal data may be anonymized for long-term statistical, historical, or research purposes.

14. INTERNATIONAL DATA TRANSFERS

- 14.1** The Conservancy recognizes that personal data must be protected regardless of where it is transferred or stored. Any transfer of personal data outside Kenya shall be done in compliance with the Data Protection Act, 2019,

15. PERSONAL DATA SHARING AND DISCLOSURE


- 15.1** The Conservancy is committed to handling personal data responsibly and will only share it with third parties when necessary, lawful, and in accordance with the Data Protection Act, 2019.
- 15.2** Data Subjects shall be informed, through a privacy notice or other means, about who their data may be shared with and for what purposes.

16. COMPLAINTS REPORTING

- 16.1** Any complaints by data subjects shall be logged with the Conservancy in writing through email at dataprotection@olpejetaconservancy.org.
- 16.2** If you have any questions about this Data Protection Policy, please contact the Data Protection Officer via email: dataprotection@olpejetaconservancy.org or Telephone: (+254) 0724 619 228 or 0725 939 35

17 MONITORING AND REVIEW

- 17.1** This Policy shall be reviewed annually or an adhoc basis in response to legislative changes and change in business operating environment.
- 17.2** Reviews will be overseen by the DPO.

PREPARED BY: _____  _____ DATE: 10/07/2025

DATA PROTECTION OFFICER



APPROVED BY: _____ DATE: 10/07/2025

CHIEF EXECUTIVE OFFICER

RATIFIED BY: _____ DATE: 07/08/2025

BOARD OF DIRECTORS

NEXT REVIEW DATE: 09.07.2026