Data Protection Policy 2023

Risk Owner	Chief Executive Officer
Approver	International Board
Review Date	June 2026

1. Purpose and objectives of the Policy

1.1. This Policy:

1.1.1. Is a formal acknowledgement that the International Board (Board) of World Animal Protection is committed to maintaining a strong personal data protection culture. The aim is to ensure that World Animal Protection (the Charity) makes every effort to manage the processing of personal data appropriately by maximising potential opportunities whilst minimising the adverse effects of risks associated with such processing.

1.1.2. Should be used to support the internal control systems of the Charity, enabling the Charity to respond to operational, strategic and financial risks regardless of whether they are internally or externally driven.

1.2. The primary objectives are:

1.2.1. To ensure that World Animal Protection's legal group (Group) have in place all necessary measures to protect the rights and freedoms of the people whose personal data we process ('data subjects'), and to minimise the risk of our causing them distress and damage.

1.2.2. To ensure that personal information is dealt with securely and in accordance with the EU and UK General Data Protection Regulations (GDPR and UK GDPR) and any other local data protection legislation.

1.2.3. To assign accountability to management and staff for the management of personal data processing within their control and provide a structured process for risk to be considered, reported and acted upon throughout the organisation.

1.2.4. To protect and minimise the Charity's exposure to data breaches.

1.2.5. To ensure that our third parties have compliant data protection safeguards and secure measures in place, whilst processing personal data on behalf of World Animal Protection.

2. Scope

2.1. This Policy applies directly to employees, contractors and consultants (Personnel) of World Animal Protection International and the Group.

2.2. It is acknowledged that Affiliates will have their own data protection frameworks monitored by their respective independent Boards and regulators. However, they are welcome to adopt in part or whole this Policy.

3. Data Protection Policy Statement

3.1. The EU General Data Protection Regulations (GDPR) and UK General Data Protection Regulation (UK GDPR) Tailored by the Data Protection Act 2018.

3.2. World Animal protection has adopted the principles of the General Data Protection Regulation as best practice to ensure that the processing of personal data does not bring the Charity into or cause distress to our supporters or disadvantage them in any way.

3.3. Those adopting this Policy outside the UK should adhere to their local legislation as prescribed whilst using the GDPR best practise principles where possible.

3.4. The Charity will regularly review and monitor the effectiveness of its Data Protection Policy, procedures and framework.

3.5. Any incidents which are considered to pose a significant threat to the Charity, financial or otherwise, will be escalated in accordance with organisational business continuity and critical incident management frameworks.

4. Organisational roles

The role of the International Board (Board)

4.1. To ensure that a culture of personal data protection is embedded throughout the Charity.

4.2. To set the level of personal data risk appetite and risk tolerance for the Charity and in specific circumstances.

4.3. To regularly review the Charity's approach to personal data protection management and approve any changes to this.

The role of the CEO and the Global Leadership Team

4.4. To ensure that this Policy is implemented throughout the organisation.

4.5. To communicate the Charity's approach to personal data protection and set standards of conduct expected of all staff.

4.6. To satisfy itself that lesser fundamental personal data risks are being actively managed and controlled.

4.7. To ensure personal data protection implications are considered in the development of business plans, budgets and when making strategic decisions.

4.8. To approve major decisions affecting the Charity's personal data risk profile or exposure.

4.9. On behalf of the Board to maintain an overview of personal data protection management and to ensure that the system of internal control is effective, this includes financial oversight, risk management, compliance with statutory frameworks and internal audit.

4.10. GLT will ensure that the Board is adequately informed of significant data protection issues and the actions undertaken to manage risks on a regular basis.

4.11. To receive reports from internal audit, external consultants, and any other relevant parties and to make recommendations to the Board relating to data protection.

The role of the Data Protection Coordinator

4.12. Provide subject matter expert knowledge to the data protection risk owner, members of the GLT and SLT and peers across the organisation.

4.13. Provide support and guidance to all Group country office data protection leads.

4.14. Provide support and guidance to International and UK employees.

4.15. Provide administrative support and management of data protection accountability documents.

4.16. Monitor data protection risk management across the Group.

4.17. Draft and review Data Protection Policy and Procedures.

4.18. Will act as a point of contact, consult and escalate high risk processing to the appropriate supervisory authority where necessary.

4.19. Co-chair data breach response team meetings.

4.20. Project management in relation to data protection matters.

The role of the Country Directors

4.21. The Country Director is the local risk owner of its country data protection and will:

4.21.1. ensure local operational personal data protection, as appropriate.

4.21.2. provide quarterly data protection reassurance reports to the GLT upon request.

4.21.3. appoint a Local office data protection lead.

The role of Functional Directors

4.22. To anticipate and consider high risk processing that involves personal data and to keep under review the assessed level of likelihood and impact of existing key risks.

4.23. To ensure that team members are fully compliant with data protection procedures when completing related tasks.

4.24. To review and sign off all high-risk processing data impact assessments (DPIAs) prior to the project / process commencing.

The role of the Data Protection Leads

4.25. Provide support and guidance to their local office employees.

4.26. Provide data protection risk management support to their Country Director.

4.27. Ensure that all data protection logs and registers are up to date.

4.28. Escalate all high-risk processing to the Data Protection Coordinator before such processing commence.

4.29. Ensure that incidents/ breaches are reported upon in a timely fashion through designated lines of reporting.

4.30. Ensure that all data subject rights requests are processed promptly within specified timeline.

4.31. Monitor any changes in local legislation and inform the Data Protection Coordinator at World Animal Protection International if these are likely to affect their ability to comply with this Policy and complimentary procedures.

4.32. Will act as a point of contact with relevant local supervisory authority, in consultation with the Director of Governance and Legal Services.

The role of the Head of IT

4.33. To provide information technology technical support and guidance.

4.34. To co- chair breach response management team meeting and support with response.

The role of the Director of Governance and Legal Services

4.35. To report all high-level data protection risks to the Board.

4.36. To provide legal guidance to the data protection leads.

4.37. To oversee the production of any legal documentations required i.e., contracts with data sharing provisions.

4.38. To manage and support the Data Protection Coordinator.

4.39. To respond to personal data queries in the absence of the Data Protection Coordinator.

All Personnel

4.40. Everyone involved with World Animal Protection plays an important role in data protection and this is not the sole responsibility of risk owner(s). Effective personal data protection will help us prevent the Charity from disrepute and potential fines. All Personnel should:

4.40.1. Identify any potential issues of data protection compliance within their work and escalate them to their line manager so appropriate remedial action can be taken as necessary.

4.40.2. Take all reasonable steps to keep personal data secure.

4.40.3. Report emerging risks or breaches that they become aware of.

4.40.4. Co-operate and respect all policies and procedures designed to minimise personal data incidents and breaches.

4.40.5. Respond promptly to any external data protection enquires received and escalate to the relevant data protection lead.

4.40.6. Ensure personal data is collected in an appropriate manner and be able to demonstrate how they have done so.

5. Procedures

Data Protection Principles

5.1. Personal data will be:

5.1.1. Processed lawfully, fairly and transparently.

5.1.2. Collected for specified, explicit and legitimate purposes.

5.1.3. Adequate, relevant and limited to what is necessary for processing.

5.1.4. Accurate and kept up to date.

5.1.5. Kept only for as long as it necessary for processing.

5.1.6. Processed in a manner that ensures its security.

Lawful processing of data

5.2. World Animal Protection Personnel will obtain personal data for one or more specified, explicit, and lawful purpose(s), and will not process such data further in any way which is incompatible with that purpose.

5.3. All offices must ensure that:

5.3.1. they determine (and document) an appropriate lawful basis before they begin processing personal data, in accordance with the conditions listed in Appendix 2.

5.3.2. they determine (and document) an appropriate lawful basis before they begin processing special categories of data in accordance with the conditions listed in Appendix 3.

5.3.3. they determine (and document) an appropriate lawful basis before they begin processing personal data related to criminal offences and convictions, in accordance with requirements of local data protection and other relevant legislation. (See Consent Procedure).

5.3.4. They complete a legitimate interest assessment to justify the use of legitimate Interest as a lawful basis for processing data. (See Legitimate Interest Procedure).

Transparency and privacy notices

5.4. Each office must provide clear, comprehensive, and accurate privacy notices to individuals from whom they are collecting personal data, explaining exactly how they will use the data. The privacy notice must meet the minimum standards for notices required by relevant data protection law.

5.5. Documented procedures must set out the minimum requirements for these notices and a log must be maintained of previous privacy notices so that each office can identify what version of a privacy notice was available to an individual when they supplied their personal data. (See Privacy Procedure).

Adequacy of data

5.6. Staff must only collect required data to fulfil the stated purpose but no more than is necessary to fulfil it. Any excessive data obtained or held must be properly and securely deleted.

Accuracy of data

5.7. Each office must ensure that it takes reasonable steps to ensure personal data is accurate, that individuals are able to easily notify the office to ask for their information to be corrected or updated and that procedures exist to ensure that no unauthorised changes are made to data.

5.8. Data must be securely deleted or destroyed if it is not reasonable to assume it is accurate or up to date.

Data retention and disposal

5.9. Each office must keep a written retention schedule and must not retain data for longer than is required by the original purpose of its acquisition.

5.10. When no longer needed for that purpose, data must be promptly and securely deleted or destroyed unless local legislation requires longer retention.

5.11. Any data no longer used, but which must be retained (e.g., for reporting and analysis), must be securely archived.

5.12. Data must not be either collected or retained on a 'just in case' basis.

5.13. Where appropriate, data may be anonymised or pseudonymised so that no living person may any longer be identified either by World Animal Protection staff or another party.

Data security and personal data breaches

5.14. All group offices must adhere to the Information Management Policy and take all other reasonable organisational and technical measures to prevent the unauthorised or illegal processing of personal data, or the accidental loss or destruction of, or damage to, personal data held by World Animal Protection, especially when it is in transit or being processed off-site.

5.15. All group offices must adhere to the personal data breach procedure that incorporates the requirements of all local data protection and other related legislation and must keep a log of breach incidents and outcomes.

5.16. Breach response will be led by the Head of IT (Equivalent within Local office), data protection leads and appropriately selected individual(s).

5.17. Designated country data protection lead will communicate all data breaches to the international data protection lead and its country director.

6. Documentation of Data Processing Activities

6.1. All World Animal Protection group offices must keep written records of their processing activities.

6.2. World Animal Protection offices must identify and document the following:

6.2.1. What personal data is being processed? Why is it important to World Animal Protection ("the purpose")? What sorts (categories) of personal data are involved? Is any of the data defined as special or sensitive under data protection law? Was the personal data obtained directly (from the "data subject") or indirectly (from someone or somewhere else)? Is the personal data shared with anyone and if so, what is the reason for this? Where is the data stored and who has access to it? What, if any, special measures are taken to make sure it is stored or transferred to others in a private and secure way? How long is the personal data kept for and why? (use record of processing template).

7. Privacy by Design

7.1. World Animal Protection offices will conduct privacy impact assessments, data protection impact assessments, or similar, as required by relevant data protection law or as a best practice approach.

7.2. Irrespective of whether there is a legal requirement in a particular country, all offices will conduct a privacy risk assessment if (as part of a new initiative involving processing of personal data) they intend to:

7.2.1. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.

7.2.2. Process special category data or criminal offence data on a large scale.

7.2.3. Systematically monitor a publicly accessible place on a large scale.

7.2.4. Use new technologies.

7.2.5. Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity, or benefit.

7.2.6. Carry out profiling on a large scale.

7.2.7. Process biometric or genetic data.

7.2.8. Combine, compare, or match data from multiple sources.

7.2.9. Process personal data without providing a privacy notice directly to the individual.

7.2.10. Process personal data in a way which involves tracking individuals' online or offline location or behaviour.

7.2.11. Process children's personal data for profiling or automated decision-making or for marketing purposes or offer online services directly to them.

7.2.12. Process personal data which could result in a risk of physical harm in the event of a security breach.

7.3. Every office must keep a register of all completed data impact assessment, highlighting the associated risk level. (see Data impact assessment procedure).

8. Third Party Management

8.1. All offices must keep an up-to-date log of all third parties that have access to or handle personal data on behalf of World Animal Protection; and must ensure that:

8.1.1. Procurement process is aligned to data protection.

8.1.2. Written contracts and agreements are in place with those parties that commit them to processing data in accordance with relevant legal requirements and with this Policy.

8.1.3. Such contracts or agreements provide for reasonable action by us or by our appointed agent, or other form of assurance, to verify that these conditions are being observed.

8.1.4. Data protection questionnaires are completed and reviewed as part of procurement due diligence before contracts are signed.

8.1.5. The contract register is updated with data protection third party information and responsibilities. (See Procurement procedure).

9. Cross-Board Data Transfer

9.1. Each office must identify all circumstances in which personal data are transferred to third countries or organisations and must, for each such transfer, ensure that it has in place a data transfer mechanism that complies with the requirements of relevant data protection law.

9.2. Each office must adhere to the term and conditions of World Animal Protection Personal data sharing agreement, when sharing data with another country office.

9.3. Each office must ensure that before entering into a contract with an international supplier / contractor to process personal data on its behalf, there are appropriate transfer safeguards in place otherwise such contract should not be signed.

9.4. Where an office identifies data transfers for which it lacks a lawful data transfer mechanism, the organisation reviews the available options and implements the most suitable mechanism promptly or ceases the processing.

9.5. If there is any doubt about the legality of transfer, the International Data Protection Lead, or local equivalent, should be consulted.

9.6. Each office must keep a record of all data protection transfer and the mechanism for the specific transfer. (See Transfer of Personal Data Procedure).

10. Children

10.1. Children need protection when World Animal Protection collects and processes their personal data because they may be less aware of the risks involved.

10.2. World Animal protection office will not process the personal data any child under the age of 16 without the written consent of a responsible adult except where local legislation stipulates a lower age.

10.3. Children between the ages over 16 years and under 18 years old would be able to give personal consent to World Animal Protection to process their data without the need for parental consent.

10.4. World Animal Protection group offices will ensure additional safeguards when processing children's personal data.

11. Data Subject Rights

11.1. All offices will ensure that they adhere to the documented procedures in place to handle requests from individuals wishing to exercise their rights as a data subject that comply with relevant data protection legislation.

11.2. All group offices must adhere to relevant procedure to handle requests from individuals wishing to see a copy of their personal data (the right to access, also known as subject access requests) and requests from individuals wishing to exercise their "right to be forgotten" (right to erasure).

11.3. World Animal Protection must observe the principles below, which may be considered as rights, irrespective of whether they have specific legal force in any country. The data subject must:

11.3.1. have access to a copy of the information we hold about them, provided free of charge and within one month of their "reasonable" request.

11.3.2. be allowed to prevent active use of their personal data for the purposes of direct marketing.

11.3.3. be able to prevent processing, which is causing, or is likely to cause, damage or distress to the data subject.

11.3.4. be able to not have decisions taken solely based on automated processing, including profiling which produces legal effects concerning the data subject or similarly significantly affects them; and be informed about the mechanics of any automated decision-making process.

11.3.5. ask for their data in a portable format where applicable.

12. Reporting

12.1. All group offices will maintain accountability logs to evidence compliance where required.

12.2. Monthly updates of all records will be shared with the international data protection lead.

12.3. A central data impact assessment register documenting all high risks processing with pending mitigations will be held in the international office.

12.4. High risk processing that requires escalation to the supervisory authority would be documented on the strategy risk register by the data protection lead (International).

12.5. A global data protection risk management performance indicator report will be sent to the Director of Governance and Legal Services quarterly by the international data protection lead.

13. Training

13.1. All group offices must ensure data protection is included as part of new staff induction.

13.2. All group offices must ensure that all staff responsible for managing data receive appropriate training and that this is regularly refreshed every year.

13.3. Accurate and up-to-date records of training should be maintained.

13.4. All staff job descriptions must clearly lay out data protection responsibilities where relevant to the role.

14. Assurance

14.1. A personal data protection risk based internal self-assessment will be completed each year approved by the GLT to ensure that risk controls remain efficient and effective.

14.2. An internal audit by the organisation's approved internal auditors will take place periodically, as part of the regular audit plan.

14.3. Quarterly report of continuing and emerging high concern on personal data risks and those where priority action is needed to effect better control will be provided will be submitted to the Director of Governance and Legal Services.

14.4. Where data protection failures can be established to intentional or systematic neglect of this Policy by an individual, this would be performance managed in accordance with the appropriate performance management policies and procedures in place.

15. Review and approval

15.1. This Policy will be subject to review every three years and will be presented to the Board via the Audit and Finance Committee.

16. Whistleblowing

16.1. Whistleblowing in relation to data protection matters will be managed in accordance with the Whistleblowing Policy.

17. Related Policies and Procedures:

17.1. Privacy Procedure, Data Breach Procedure, Data Retention Procedure, Data Impact Assessment Procedure, Procurement Procedure, Data subject access request Procedure, Restriction and Objection request Procedure, Personal data erasure request Procedure, Consent procedure, Consent, Unstructured data Procedure, Data sharing and transfer procedure, Social Media Guidance, Complaints Policy and data Classification Procedure.

18. Relevant Legislation:

18.1. General Data Protection Regulation 2018(GDPR), Data Protection Act 2018(UK), Personal Data Protection Act 2019(Thailand PDPA), Data Protection Act 2019 (Kenya), The Federal Privacy Act 1988 (Australia), Law No. 7975, the Undisclosed Information Law and Law No. 8968, Protection in the Handling of the Personal Data of Individuals (Costa Rica),

Version control:

Version	Amendments	Approved by	Date
1	New draft to incorporate group office's legislation.	International Board	29/09/20
2	New draft to include the role of Director of Governance and Legal, UK GDPR.	International Board	15 June 2023

1. Appendix 1

Definitions

Anonymisation / pseudonymisation: are data management procedures by which personally identifiable information fields within a data record are either permanently removed (anonymisation) or replaced by one or more artificial identifiers, or pseudonyms (pseudonymisation).

Cross-border transfer: in European data protection law or similar local law, this relates to transfer of personal data outside the European Union or related country, to third countries or international organisations; such transfers are only lawful if certain safeguards are in place.

Data: is defined as structured information.

Personal data: is any information relating to a living individual who can be directly or indirectly identified from it. This includes name, address, contact details but could also include two or more non-specific pieces of information that when combined could identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator, and other descriptors.

Special categories of data / sensitive data: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and a natural person's sex life or sexual orientation. In Kenya, this has been extended to include conscience, criminal records, Property details and Family details such as names of the person's children, parents, or spouse.

Data controller: a controller determines the purposes and means of processing personal data, e.g., a Charity is the controller of the employee and supporter data it processes.

Data owner: the person in any business unit (country/functional department/section) who has primary responsibility for the effective and legal management of the personal data they hold.

Data processor: a processor carries out specific tasks (data processing activities) on behalf of (and on the instructions of) the controller under a binding contract.

Data portability: is the ability to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Data protection: This is the process by which individuals are protected from the improper management of data about them by governments, organisations, and others, and by which their privacy and rights in respect of information about them are safeguarded.

Data subject: an individual who is the subject of personal data; this excludes people who have died or who cannot be identified or distinguished from others. It would include current, former staff, trustees, volunteers, applicants, donors and supporters, representatives of partner or target organisations, and other contacts.

Data processing: means doing something with personal data including collecting, storing, using, altering, amending, creating, transferring, sharing, archiving, analysing, reporting on, deleting data.

Filing system: any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy: freedom from unauthorised disclosure of an individual's personal data or information.

Privacy notice: this is a statement made, ideally, when collecting personal data, which should give the subject clear and accurate information about how the data will be used, a consent statement (in the case of sending marketing information to supporters) and who their data may be shared with. The result should be that an individual's personal data is not used in ways which they would not expect.

Third party: a natural or legal person, other than the data subject, controller or processor, who, under

the direct authority of the controller or processor, is authorised to process personal data.

2. Appendix 2

Conditions of fair processing of personal data

1. The conditions attached to fair processing include the following:
   - Consent: you can show that an individual has performance a clear affirmative action (such as saying 'yes' to a question or ticking an opt-in bot) to allow you to process their personal data for a specific purpose.
   - Contract: the processing is necessary for a contract you have with the individual or because they have asked you to take specific steps before entering into a contract.
   - Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
   - Vital interests: the processing is necessary to protect someone's life.
   - Public interest: the processing is necessary for you to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
   - Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless the interests or rights and freedoms of the individual override those interests.

3. Appendix 3

Conditions of fair processing of special categories of data

1. The conditions attached to fair processing of special category data includes the following:

- The individual who the sensitive personal data is about has given explicit consent to the processing.

- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of an individual (in a case where the individual's consent cannot be given or reasonably obtained) or another person (in a case where the individual's consent has been unreasonably withheld).
- The processing is carried out by some types of not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. This condition is quite restrictive and does not apply to most charities.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings, for obtaining legal advice, or for otherwise establishing, exercising or defending legal rights.
- The processing is necessary for administering justice or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of the individuals.
- Processing to prevent or detect a crime where seeking consent would inhibit the ability to do so.