# Data Protection Policy

<table>
<thead>
<tr>
<th>Version number</th>
<th>2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by International Board</td>
<td>6 June 2018</td>
</tr>
<tr>
<td>Next review</td>
<td>June 2020</td>
</tr>
</tbody>
</table>

World Animal Protection is a global organisation which comprises affiliated entities working together in support of an agreed global strategy, and bound through collaboration agreements to adhere to a set of corporate policies which reflect our principles and values.

## I Scope

1. All World Animal Protection staff, consultants, board members and volunteers. Staff means all employees of World Animal Protection, whether permanent, temporary or interim, in all its branches and subsidiaries and in all affiliated entities. Where the term ‘staff’ is used, it should be taken to mean anyone to whom the policy applies unless otherwise specified.

2. All third parties that process personal data on World Animal Protection’s behalf.

## II The Policy

This updated and revised version of World Animal Protection’s data protection policy is designed primarily to ensure that globally we 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’; and secondarily, to ensure that we – as an organisation and as individual employees – are protected as far as possible against liability arising from the possible mismanagement of all personal data. See Appendix 1 for what is meant by personal data. The policy should be read in conjunction with all our other global policies.

The policy is intended to meet the broad requirements of applicable legislation and regulations in all jurisdictions in which we are represented; all offices are required to observe their local data protection and privacy legislation, whether or not it is covered in this policy.

All staff are responsible for managing personal data we collect in a proper manner, and, as importantly, for being able to demonstrate that they have done so. Breaches of this policy may therefore be treated under World Animal Protection disciplinary procedures and potentially under criminal or civil law.

The policy covers the processing of all personal data by World Protection staff, and applies also to all other organisations which we contract to carry out any of the processing on our behalf. Where the term “data” is used without qualification, this should be understood to mean personal data.
Enabling and accountability measures

Data protection legislation and policy

1. Every World Animal Protection office must be aware of the key features of its local data protection legislation. They must monitor any changes in it and inform the Data Protection Lead at World Animal Protection International if these are likely to affect their ability to comply with this policy.

2. Every World Animal Protection office must have in place documented procedures that support this Policy and any additional requirements relating to local data protection legislation.

Data protection lead

3. All World Animal Protection offices must nominate a key contact for Data Protection (a "Local Data Protection Lead") to be responsible for liaising as necessary with their national data protection authorities and with World Animal Protection International, and for monitoring and demonstrating local compliance with this policy and all relevant local data protection legislation.

4. The Data Protection Lead at World Animal Protection International (the "International Data Protection Lead") will monitor data protection compliance globally, and may make decisions on high-risk processing.

Documentation of data processing activities

5. Every World Animal Protection office must keep written records of their processing activities.

6. All World Animal Protection offices must identify and document the following: 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?

Third-parties

7. 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:
   - 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
   - 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.

Privacy by design

8. All offices will conduct privacy impact assessments, data protection impact assessments, or similar, as required by relevant data protection law.
9. Irrespective of whether there is a legal requirement in any 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:
   a. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
   b. Process special category data or criminal offence data on a large scale.
   c. Systematically monitor a publicly accessible place on a large scale.
   d. Use new technologies.
   e. Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit.
   f. Carry out profiling on a large scale.
   g. Process biometric or genetic data.
   h. Combine, compare or match data from multiple sources.
   i. Process personal data without providing a privacy notice directly to the individual.
   j. Process personal data in a way which involves tracking individuals’ online or offline location or behaviour.
   k. Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
   l. Process personal data which could result in a risk of physical harm in the event of a security breach.

Data protection training

10. All offices must ensure data protection training is included as part of the induction of new staff, and ensure that all staff responsible for managing data receive appropriate training and that this is regularly refreshed not less than every two years.

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

12. Staff job descriptions must clearly lay out data protection responsibilities where relevant to the role.

Children

13. Children need particular protection when World Animal Protection collects and processes their personal data because they may be less aware of the risks involved. Each office will ensure that it has adequate internal policies and documented procedures regarding processing of personal data of children to comply with relevant data protection and other relevant legislation, including but not limited to appropriate procedures for obtaining parental consent to process children’s personal data, where required.

Cross-border transfers

14. 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.
15. 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.

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

**Principles of data protection**

17. Personal data will be:
   a. Processed lawfully, fairly and transparently
   b. Collected for specified, explicit and legitimate purposes
   c. Adequate, relevant and limited to what is necessary for processing
   d. Accurate and kept up to date
   e. Kept only for as long as it necessary for processing
   f. Processed in a manner that ensures its security.

**Lawful processing of data**

18. World Animal Protection staff 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.

19. All offices must ensure that:
   a. they determine (and document) an appropriate lawful basis before they begin processing personal data, in accordance with the conditions listed in Appendix 2.
   b. 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.
   c. 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.

**Transparency and privacy notices**

20. 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.

21. 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 is able to identify what version of a privacy notice was available to an individual when they supplied their personal data.
Adequacy of data

22. Staff must collect sufficient 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

23. 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. 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

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

25. Any data no longer used, but which has to be retained (e.g. for reporting and analysis), must be securely archived. Data must not be either collected or retained on a ‘just in case’ basis.

26. 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 subject rights

27. All offices will ensure that they have 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.

28. All offices must have a documented 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).

29. World Animal Protection must observe the principles below, which may be considered as rights, irrespective of whether they have specific legal force in any particular country. The data subject must:
   • have access to a copy of the information we hold about them, provided free of charge and within one month of their “reasonable” request.
   • be allowed to prevent active use of their personal data for the purposes of direct marketing.
   • be able to prevent processing which is causing, or is likely to cause, damage or distress to the data subject.
   • 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.
• be able, in certain circumstances, to have data corrected, blocked, erased or destroyed; and may in some countries and circumstances be able to claim compensation for a breach of data protection legislation by World Animal Protection.

Data security and personal data breaches

30. 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 offsite.

31. All offices must have a documented personal data breach procedure that incorporates the requirements of local data protection and other related legislation and must keep a log of breach incidents and outcomes.
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).

Crossborder transfer: in European data protection law, this relates to transfer of personal data outside the European Union, 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: 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.

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 and former staff.
and 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.
Appendix 2

Conditions of fair processing of personal data

1. The conditions attached to §19a include the following:
   - Consent: you can show that an individual has performed a clear affirmative action (such as saying “yes” to a question or ticking an opt-in box) 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 task: the processing is necessary for you to perform a task in the public interest or for your 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.

Appendix 3

Conditions of fair processing of special categories of data

2. The conditions attached to §19b include 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:
     - the 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 otherwise for 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 individuals.
   - Processing to prevent or detect a crime where seeking consent would inhibit the ability to do so.