CIC Data Protection Policy

May 2018

The following document is based on the IUCN Data Protection Policy (2018), which the CIC, as an IUCN member, has modified for its purposes. The aim of this Policy is to communicate the general principles and guidelines applicable to the protection of personal data.

Contents

1. Definitions
2. Introduction
3. Applicability of the Policy
4. Principles of data processing
5. Rights of the Data Subjects
6. Commitments
7. Implementation
8. Modification of the Policy

Definitions

Anonymisation means using techniques that seek to conceal the identity and thus identifiers of any nature. Identifiers can apply to any natural or legal person, living or dead, including their dependents, ascendants and descendants. Included are other related persons, direct or through interaction.

Data Breach means a breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of, or access to – Personal Data transmitted, stored or otherwise processed.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the 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 a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

Data Transfer mean any act that makes Personal Data accessible, whether on paper, via electronic means or the internet, or any other method to any Third Party not linked in a way or another to the CIC.

Personal Data means any information relating to an identified or identifiable natural person. This may include an identifier such as a name or audio-visual materials, an identification number, location data, or an online identifier; it may also mean information that is linked specifically to the physical, physiological, genetic, mental, economic, cultural, or social identity of a Data Subject. The term also includes data identifying or capable of identifying human remains.

Processing means any operation or set of operations – by automated and other means – that is performed upon Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmitting, disseminating or otherwise making available, aligning or combining, or erasing.

Recipient means third party, public authority, agency, or other body – that is, someone or something other than the Data Subject or the CIC – to which the Personal Data is disclosed.

Sensitive Personal Data means specific Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic Data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third Country means any other country or jurisdiction outside of Austria or Hungary. Third Party means a natural or legal person, public authority, agency, or body other than the Data Subject or the CIC.

1. Introduction

The CIC is committed to safeguarding and protecting Personal Data of private individuals. The CIC is aware of the risks involved, and of the importance of having appropriate data protection standards in place. In the scope of its mission, which consists of promoting – across the globe – sustainable hunting to conserve wildlife and wild lands, supporting communities, and preserving our hunting heritage, the CIC needs to gather and use certain information about individuals. These can include members, donors, suppliers, business contacts, visitors to the CIC building, employees, and other people the organisation has a relationship with or may need to contact. Safeguarding the Personal Data of all these persons is an essential aspect of protecting people's lives, integrity, and dignity. The Processing of Personal Data touches all areas of its activity, whether operational or administrative. This Policy describes the principles to be followed when Processing Personal Data. It also describes how they should be implemented and what needs to be done in case of a Data Transfer and Personal Data Breach event in order to comply with reporting requirements. The aim of this Policy is to a) comply with national and international data protection laws and regulations, b) protect the rights of data subjects c) protect the CIC from the risks of Data Breach, and d) protect the CIC from undesired legal sanctions which may include hefty fines. Defined terms appear in capital letters throughout this Policy and are defined in the Definitions section.

2. Applicability of the Policy

This Policy applies to staff members of the CIC (including hosted staff), regardless of location and office type. It also applies to volunteers working for the CIC, and individuals seconded by other organizations to the CIC collectively referred to as "CIC Staff" and to carriers of official CIC mandates (such as elected Heads of National CIC Delegations, leadership of CIC Divisions, Certified CIC Measurers, Senior International Trophy Judges, etc.). Further, it applies to the CIC as a Data Controller or Data Processor with respect to Personal Data relating to Data subjects. This Policy comprises the internationally accepted data protection principles without replacing the existing national laws. It supplements the national data protection laws. The relevant national law will take precedence in the event that it conflicts with this Policy or it has stricter mandatory requirements than this Policy. In particular, the reporting requirements for data Processing under applicable national laws must be observed. The content of this Policy must also be observed in the absence of corresponding national legislation.

3. Principles of data processing

3.1 Legitimate and fair Processing

The CIC processes Personal Data in a lawful and fair manner in relation to the Data Subject. The CIC only processes Personal Data with respect to this Policy and applicable laws. In order to do so the CIC ensures that there exists a legal basis of Processing Personal Data such as the following:

3.1.1 Consent of the Data Subject

The CIC ensures that consent is obtained from the Data Subject prior to Processing Personal Data. This Consent is obtained in writing or electronically for the purposes of documentation and is valid only if given voluntarily. If, for any reason, the consent of the Data Subject is not given before Processing Personal Data, it should be secured in writing as soon as possible after the beginning of the Processing. The CIC takes particular care in Processing Sensitive Personal Data and will only do so with prior written consent of the Data Subject.

3.1.2 Legitimate Interest of the CIC

The CIC may process Personal Data without express consent if it is necessary to enforce a legitimate interest of the CIC.

3.1.3 Contractual obligation

The CIC may process Personal Data in order to enforce a contract entered into with the Data Subject or to comply with a contractual obligation.

3.1.4 Compliance with a legal obligation

In other cases, the Processing of Personal Data may be necessary to comply with applicable law.

3.1.5 Public interest

The CIC may process Personal Data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the CIC through its mandate or Statutes.

3.2 Transparency

The CIC processes Personal Data in a transparent manner.

Communications with the Data Subject must be in clear and plain language, easily accessible and easy to understand. CIC Staff and carriers of official mandates in the CIC must provide the Data Subject with sufficient information about the data Processing when Personal Data is obtained. The minimum information to be provided is included **in section 4.1 Right to receive information.**

CIC Staff and carriers of official CIC mandates Processing Personal Data will decide how this information is to be communicated after taking into account security measures and the urgency of Processing.

3.3 Restriction to a specific purpose

When collecting Personal Data, CIC Staff and carriers of official CIC mandates in charge determine the specific purpose(s) for which data are processed, and only processes them for those purposes. All Personal Data collected should be clearly documented including the purpose for collection.

3.4 Adequate and relevant data

The Personal Data handled by the CIC must be adequate, relevant, and limited to what is necessary in relation to the purpose for which it is processed. This means that CIC Staff and carriers of official CIC mandates should not process Personal Data unless it is necessary to process it in order to achieve the purpose for which it was obtained.

3.5 Accuracy

CIC Staff and carriers of official CIC mandates must ensure that Personal Data kept on file is correct and kept up to date. Inaccurate or incomplete Personal Data should be rectified or deleted. The exception to this principle would be in case a legitimate interest exists to retain Personal Data. Historical data, accurate at the time of collection can be kept for as long as it is required to be kept. Once historical data is no longer necessary it should be deleted.

3.6 Integrity and confidentiality

CIC Staff and carriers of official CIC mandates must treat Personal Data in a confidential manner. They must ensure that Personal Data is securely stored with suitable organizational and technical measures to prevent unauthorized or illegal Processing.

3.7 Retention, destruction and archiving of data

The CIC keeps Personal Data for as long as it is necessary to perform its activities and as is required by applicable law. Personal Data not useful for the CIC should be deleted unless if required by national legislation to be retained for a certain period of time. The CIC will also delete Personal Data if the Data Subject withdraws his or her consent for Processing unless there exists another legal basis of Processing the Personal Data.

The CIC may store Personal Data for archiving purposes for a determined period compatible with applicable laws.

4. Rights of the Data Subjects

The CIC respects rights conferred to Data Subjects to ensure protection of Personal Data. These rights include:

4.1 Right to receive information

At a minimum, CIC Staff and carriers of official CIC mandates must provide the Data Subject with the following information when Personal Data is obtained:

- whether the CIC is the Data Controller;
- the purpose of Data Processing;
- third-parties to whom the data might be transmitted;

- the existence of this present Policy;
- the focal point for questions/concerns or complaints.

This information should be communicated to the Data Subject even in cases where the Personal Data was not obtained directly from the Data Subject.

4.2 Right to access

The Data Subject may request which Personal Data relating to him or her has been collected and stored, how the Personal Data was collected, and for what purpose. Requests from the Data Subject wishing to verify what Personal Data is held by the CIC must be submitted in writing to the Headquarters (office@cic-wildlife.org).

Disclosure of Personal Data should not be automatic. CIC Staff and carriers of official CIC mandates must consider all the circumstances surrounding the request for access and any restrictions to access that may be applicable. Access to Personal Data will only be given to the Data Subject if his or her identity can be verified.

4.3 Right to rectification

If Personal Data is incorrect or incomplete, the Data Subject can request that it be corrected or supplemented. This will only be considered if the identity of the Data Subject can be verified. Upon verification of the allegation, the CIC will make the necessary change(s). In certain circumstances historical data may need to be kept in accordance with section 3.5 Accuracy.

4.4 Right to erasure – "Right to be forgotten"

The Data Subject may request his or her Personal Data to be deleted if the Processing of such Personal Data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the Data Processing has lapsed or has ceased to be applicable for other reasons. However, the right to erasure does not apply, and Personal Data will continue to be retained:

- for the implementation of the Mission of the CIC;
- if it serves a public interest;
- for historical, statistical, and scientific purposes; or
- for the establishment, exercise, or defence of legal claims;
- for other legitimate interests (legal and financial).

4.5 Right to Personal Data portability

The Data Subject has the right to receive his or her Personal Data in a structured, commonly used and machine-readable format and has the right to transfer such Personal Data to another Data Controller provided the Processing was based on consent or was necessary for the performance of a contract and was carried out by automated means. Where technically feasible the Data Subject may request the CIC to transfer his or her Personal Data to another Data Controller.

4.6 Right to object

The Data Subject may object at any time, on compelling legitimate grounds relating to their particular situation, to the Processing of Personal Data concerning them. Such objection will be accepted if the fundamental rights and freedoms of the Data Subject in question outweigh the CIC's legitimate interests, or the public interest. An objection to Personal Data Processing does not apply if a legal, contractual or financial provision requires the Personal Data to be processed.

4.7. Right to restriction of processing

The Data Subject has the right to restrict the Processing of his or her personal data where there exists a particular reason for the restriction. This means that the Data Subject can limit the way that an organisation uses his or her Personal Data. This may be because:

- the accuracy of the Personal Data is contested by the Data Subject;
- the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
- The CIC no longer needs the Personal Data for the purposes of the Processing, but the Personal Data is required by the Data Subject for the establishment, exercise, or defence of legal claims;
- the Data Subject has objected to the Processing pending the verification whether the legitimate grounds of the CIC override those of the Data Subject.

4.8. Automated individual decision-making, including profiling

The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

5. CIC commitments

5.1 Responsibility/Accountability

It is the responsibility of the CIC Staff and carriers of official CIC mandates to ensure that Personal Data processed for or on behalf of the CIC, is in compliance with this Policy.

5.2 Arrangements with our partners (including consultants)

In particular, when the CIC collaborates with another entity in Processing Personal Data, CIC Staff and carriers of official CIC mandates should ensure that the responsibilities of all the parties concerned as described in this Policy are outlined very clearly and set out in a contract or other legally binding arrangement.

5.3 Data protection by design and by default

In particular, while designing a database and drafting procedures for collecting Personal Data, the principles of data Processing and the rights of data subjects stipulated in the present Policy must be taken into account and incorporated to the greatest extent possible.

5.4 Data security and storage

CIC Staff and carriers of official CIC mandates should process Personal Data in a manner that ensures an appropriate degree of security. This includes prevention of unauthorized access to or use of Personal Data and the equipment used for data Processing. This relates in particular to access rights to databases, physical security, computer security and network security, the duty of discretion and the conduct of all CIC Staff and carriers of official CIC mandates who have access to Personal Data.

The CIC undertakes to store electronic equipment and Personal Data safely. The CIC has implemented technical measures to ensure that Personal Data stored electronically is protected from unauthorised access, accidental deletion, and malicious hacking attempts. In particular, Personal Data should never be saved directly on laptops or other mobile devices like tablets, smart phones, USB Drives, DVDs, etc. and should be protected by strong passwords.

When Personal Data is stored physically or when Personal Data usually stored electronically has been printed it should be kept in a physically secure place where unauthorised people cannot see it (e.g. in a locked drawer or filing cabinet). Papers and printouts containing Personal Data should not be left where unauthorised people could access them (e.g. on a printer) and should be shredded and disposed of securely when no longer required.

In any case, when retention of Personal Data is no longer necessary, all records should be securely destroyed or anonymised. The Anonymization of the Personal Data is allowed if this is necessary to the CIC's Mission.

5.5 Newsletters

It is the responsibility of CIC Staff in charge of newsletters to ensure that express consent is obtained from the Data Subjects and recorded. Where the Data Subject has not given his or her express consent to receive newsletters, his or her Personal Data should be deleted.

5.6 Data Breaches

Any breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of, or access to – Personal Data transmitted, stored or otherwise processed must always be reported in writing to the Headquarters (office@cic-wildlife.org). In the event of a Data Breach, the Director General will ensure there is an appropriate response which means:

5.6.1 Establishing a team to investigate the Data Breach, and develop remedial plan.

5.6.2 Informing the persons affected of the Data Breach without undue delay according to international or local regulations;

5.6.3 Informing the relevant local authorities according to international or local Regulations.

5.7 No commercial use of Personal Data

The CIC does not make commercial use of Personal Data. In case the CIC needs to use Personal Data for commercial purpose in the scope of its mission, the CIC will collect the formal consent of the Data Subject prior to any such usage. CIC Staff and carriers of official CIC mandates will keep this consent on file with the Personal Data.

5.8 Data Transfer

5.8.1 External Data Transfer

The CIC ensures that Personal Data is only transferred to jurisdictions or international organizations that ensure adequate level of protection. Should it be necessary to transfer Personal Data to a Third Country or an international organization that does not provide adequate level of protection, the CIC will ensure that it maintains appropriate safeguards such as entering into appropriate contractual clauses in order to safeguard Personal Data. When transferring Personal Data to a Third Party, CIC Staff and carriers of official CIC mandates must ensure that:

- the Recipient will apply a protection level equivalent or higher to this Policy;
- appropriate safeguards are put in place where a Third Country or an international organization does not provide adequate level of protection;
- processing by the Recipient is restricted to the purpose authorized by the CIC and;
- data transfer is compatible with the reasonable expectations of the Data Subject.

5.8.2 Data Transfer within the CIC systems

For the sake of clarification, Data Transfer between CIC Staff in different locations are permitted and do not necessitate a written agreement provided the principles set out in this Policy are respected.

6. Implementation

6.1 Effective implementation

Effective implementation of these rules is crucial to ensure that individuals are able to benefit from the protection afforded by them. It is the responsibility of the CIC and CIC Staff as well as carriers of official CIC mandates to ensure implementation of the principles.

6.2 Authorized Processing

Personal Data Processing should be in accordance with the purposes authorized by the CIC in the course of executing professional duties. CIC Staff and carriers of official CIC mandates must not use CIC Personal Data for private or commercial purposes or disclose it to unauthorized persons.

6.3 Reporting of non-compliance

Allegations of non-compliance with this Policy should be reported in writing to the Headquarters (office@cic-wildlife.org). CIC Staff and carriers of official CIC mandates who do not adhere to this Policy may be subject to disciplinary measures.

6.4 Consultation and means of communication

CIC Staff and carriers of official CIC mandates may consult with their manager/CIC Legal Counsel, if they are unsure of any aspects of this Policy.

Personal Data requests from Data Subjects (e.g. for access, rectification, or deletion of data) should be submitted in writing to the Headquarters (office@cic-wildlife.org). Any Personal Data requests received via email or in hard copy should be forwarded to office@cic-wildlife.org.

The CIC will ensure practical communication and training from time to time.

7. Modification of the Policy

This Policy may be updated from time to time. Any modifications to this Policy must be in writing and approved by the CIC Executive Committee.