WHC Conservation Certification Data Governance

April 1, 2019

This document outlines data governance considerations for data entered into WHC's Conservation Certification website.

Contents

Data Classification

To ensure that data is handled appropriately, data pertaining to Conservation Certification is classified into one of the following five categories. These categories are designed to streamline data access and protections. In addition to descriptions, examples of each data type are included for illustrative purposes (these examples are not intended to be a definitive or exhaustive list of data in the category).

Personal

Personal information is information that can be used to identify (or de-anonymize) a natural person. This information is generally operational in nature but falls into a separate category to facilitate efficiently supporting a data subject's request for erasure should such a request be received. This right to erasure is part of the European Union's General Data Protection Regulation (GDPR).

Examples of personal data:

- Name (first and last)
- Phone number
- Email address
- Job title
- IP Address

Operational

Data that is important for business functionality but is not to be used beyond that (i.e. should not be made public or available to external parties without pseudonymization). This data is key to WHC's support of applicants and data analysis but the level of detail of the information indicates that it should not be shared externally with anyone other than the company that provided the data.

Examples of Operational data:

- Most application question answers
- Reviewer scores and comments

Public

Information that is made publicly available or can be used publicly by WHC. Individual requests to not make information public will be accommodated to the extent that the request is feasible (i.e. if such a request does not impose a significant time/cost burden on WHC). As part of the Conservation Certification website's terms of use, applicants confirm that they have received all appropriate releases/permissions for photos entered into the website to be used publicly (unless otherwise noted).

Example of Public data:

- Photos

Confidential

Data that should remain encrypted or otherwise obscured/hidden (in whole or in part) so that WHC staff do not have access to it.

Data subjects who provide WHC staff with confidential information, or expressly request that WHC staff handle such information, acknowledge that in doing so they give WHC staff permission to access that information. For example, if an applicant wishes to pay an invoice by credit card over the phone, WHC staff can input the applicant's credit card into the system on their behalf. In doing so, WHC staff will have temporary access to confidential credit card information. WHC staff will not maintain separate records of this information and, once input, it is subject to the same protections as credit card data entered directly by the applicant.

Examples of Confidential data:

- Credit card information (partially obscured)
- Passwords (completely inaccessible)

Status Dependent

Some data has different permissions depending on the status indicated by that data or associated data. Most notably, this applies to general information about programs that is shared publicly through the WHC Index (unless otherwise requested). This general information about a program, its certification status and projects. however, is not publicly available after a program loses certification.

Information about programs that were formerly certified is not made available to the general public. Similarly, information about projects included in an application is only included in the public facing program description if the project was qualifying. Generally, Status Dependent information will change between Public and Operational classifications.

Examples of Status Dependent data:

- Organization, Subsidiary, and Program Names
- Program Description (written summary about the facility and efforts taking place there)
- Site location (visible on a map)
- Certification status
- List of qualifying projects

Data Ownership

Data provided to WHC (through the Conservation Certification website or other means) is considered owned by WHC. This data will be used by WHC as part of its business. WHC's use of the data will follow the Data Categorization and Data Pseudonymization outlined in this document. No data will be sold to an external party.

Data Access

Outside of WHC staff, certification related data is generally managed at the program/application level. Each program is affiliated with an organization. The organization has the right and responsibility to manage the data and who has access to the data (outside of the access afforded to WHC staff). Access to data can be provided to employees, contractors, partners, etc. of the organization (collectively referred to as appointees). The access awarded to appointees is at the organization's discretion. Based on an appointee's permission levels, they can add, remove, or change permission levels for themselves or others within the Conservation Certification website to determine who (outside of WHC) will have access to the data. Data exported from the website falls under the same rules and it is up to the organization to determine appointees for exported data as well.

Data Attribution

Data exported from the website must be attributed to the Wildlife Habitat Council's Conservation Certification. WHC reserves the right to request that a formal agreement that describes data attribution be signed by the party that will be using the data.

Data Transfer

If the site that a program is based at is sold, merged, or acquired, the certification and its associated data (both past and current) can be transferred to the new owner of the site. When WHC is notified of such a change, best efforts will be made to identify an appropriate contact with the new owner. Whether an appropriate contact for the new owner is identified by the old owner or by WHC, the program may be transferred to the new owner.

Transfer of the program places the program under a new organization in the Conservation Certification website. The new organization then has the right and responsibility to manage the data and who has access to the data (outside of the access afforded to WHC staff). This includes removing contacts no longer associated with the program. WHC can provide assistance with updating permissions if such assistance is needed.

WHC reserves the right to not transfer a program to a new owner. The old owner may send a written request to WHC to not transfer a program to a new owner, which will be carefully considered by WHC when determining if a program should be transferred.

If a new owner or appropriate contact with a new owner cannot be identified, WHC will not transfer the program and its data to another user. Instead, the program may be deactivated. If the program is currently certified, WHC reserves the right to remove the certified designation before the certification expires if it has been confirmed that the existing organization no longer owns the program.

Data Security

The WHC Conservation Certification website utilizes SmartSimple® software. SmartSimple has robust security measures and provides public access to their Security, Privacy, and Architecture documentation. This documentation provides detailed descriptions of various potential risks and the steps that are taken to mitigate these risks. Regular monitoring and tools are used to help identify potential threats and potential incidents such as data breaches.

In the event that a data breach occurs, SmartSimple will notify WHC promptly upon detection. WHC will then notify affected users as quickly as possible about the potential of data being compromised.

Data Management

The following data management policies help WHC ensure that data is cleaned, maintained, and used appropriately.

Personal Data Management

In addition to deleting personal information as requested, WHC will take additional measures to ensure that personal information is not retained for longer than it is needed. Personal information associated with an account that has not been used for 6 years will be automatically archived. If the data is still not needed after an additional 4 years in archive, the personal data will be deleted.

Data Quality Management

The usefulness of data is largely determined by the quality and integrity of the data. As a result, WHC will periodically review data and take measures to remedy any data issues that are discovered. Issues that can impact data quality and integrity vary, and can include issues with completeness, validity, consistency, etc. As a result, WHC may take a variety of corrective actions. For example, if an address is missing, WHC may populate it to ensure the completeness of that data.

Data Pseudonymization

Requests for data that is not publicly available (either Public or Status Dependent data) from external parties looking for broad data sets (i.e. data inclusive of multiple organizations) will be reviewed by the Certification Department on a case-by-case basis. An example of the use of pseudonymized data would be data provided for a research study.

If the request is approved, the Certification Department will pseudonymize the data as much as possible. Pseudonymized data ensures that the data cannot be attributed to a data subject without the use of additional information (anonymized data would irreversibly remove the ability to attribute data to a data subject. Pseudonymized data would enable WHC to later determine data subjects by tying the data to other internal (Operational) data.

Data request by those outside of an organization will often be restricted to fields that do not have any identifying information (e.g. checkboxes, numeric fields, drop-downs). If a data request includes data that might have identifying information within it (i.e. text fields and uploads), WHC will ensure the recipient of the self-identifying data does not share such information without first anonymizing it.

Data Deletion

Data can be deleted by different entities. In keeping with GDPR, data subjects may request that their personal data be deleted at any time (and request evidence that it has been completed). Data backups are on a 90-day cycle, so data will be completely deleted 90 days after a deletion occurs.

Additionally, based on the permission levels provided in the Conservation Certification website, applicants and associated persons may directly delete data pertaining to programs before data is submitted in a certification application.

Users may request that an organization or program be deleted, and WHC will accommodate such requests if they do not impact WHC's data/records (e.g. accidental duplication of a program). Data from submitted applications can not be edited or deleted. WHC maintains data from applications to use in metrics, data analysis, assisting applicants, etc. and it plays an important role in WHC's business. The use of this data is governed by the parameters outlined in this document (e.g. Data Pseudonymization, Data Classification). While WHC generally maintains data, WHC is not responsible for any data loss and reserves the right to delete data under appropriate circumstances.