

Sovereign Climate Data

Ten operational principles defining what it means for climate data to be sovereign, verifiable, AI-legible, and legally defensible in 2026.

- [Sovereign Climate Data — Overview](#)
- [Technical Quality](#)
 - [P01 — Verifiability by Design](#)
 - [P02 — FAIR Data Standards](#)
 - [P03 — Full Provenance Traceability](#)
 - [P04 — Methodological Sovereignty](#)
 - [P05 — Temporal Persistence and Baseline Integrity](#)
- [Digital Sovereignty](#)
 - [P06 — AI-Legibility](#)
 - [P07 — Third-Party Anchoring](#)
- [Governance and Social Legitimacy](#)
 - [P08 — Community and Indigenous Data Consent](#)
 - [P09 — Regulatory Stack Alignment](#)
 - [P10 — Resilience, Security and Data Governance](#)
- [API Reference](#)

Sovereign Climate Data — Overview

Sovereign Climate Data Principles

The definitive framework for verifiable, AI-legible, and legally defensible climate data — built for LATAM, aligned to global standards.

Version 1.0.0 Updated 2026-05-26 10 Principles CC-BY 4.0 AI-Legible BookStack REST API
10
Core Principles
3
Principle Layers
(Technical · Digital · Governance)
5
Regulatory Frameworks
Covered (2026 stack)

What is Sovereign Climate Data?

Sovereign climate data is environmental and impact data that an organisation **owns, controls, and can defend independently** — regardless of which platforms, vendors, or partnerships it uses. In 2026, with the EU Green Claims Directive, CBAM, ISSB S2 mandates across LATAM, and Article 6 carbon market rules all entering force simultaneously, sovereign climate data has shifted from a competitive advantage to a baseline legal requirement.

This framework defines ten principles across three layers:

- **Technical Quality** (P1–P5): The data is correct, traceable, and yours to keep.
- **Digital Sovereignty** (P6–P7): The data is discoverable, citable, and AI-legible.
- **Governance and Social Legitimacy** (P8–P10): The data is ethically grounded, regulation-ready, and institutionally resilient.

Principles at a Glance

ID	Principle	Layer	Primary Standard
----	-----------	-------	------------------

SCD-P01	<u>Verifiability by Design</u> <i>If it cannot be checked, it does not count.</i>	TECHNICAL	EU Directive 2024/825 (Green Claims / EmpCo) — Art. 5, 6
SCD-P02	<u>FAIR Data Standards</u> <i>Findable. Accessible. Interoperable. Reusable.</i>	TECHNICAL	FAIR Data Principles — Wilkinson et al., Scientific Data (2016)
SCD-P03	<u>Full Provenance Traceability</u> <i>Without provenance, a number is a narrative.</i>	TECHNICAL	Verra VM0042 Methodology (2026 update) — Section 5 (MRV requirements)
SCD-P04	<u>Methodological Sovereignty</u> <i>You own your data only if you own your method.</i>	TECHNICAL	IPCC AR6 — Annex II (Methodologies for GHG inventories)
SCD-P05	<u>Temporal Persistence and Baseline Integrity</u> <i>A result without a baseline is a claim without evidence.</i>	TECHNICAL	ISSB IFRS S2 — Para. 22–28 (Transition provisions and comparatives)
SCD-P06	<u>AI-Legibility</u> <i>If an AI agent cannot cite you, you do not exist.</i>	DIGITAL	EU CSRD — Art. 8 (machine-readable XBRL tagging requirement)
SCD-P07	<u>Third-Party Anchoring</u> <i>Your claim is only as strong as its external anchor.</i>	DIGITAL	CBAM Regulation EU 2023/956 — Art. 10(3) (Accredited VVB requirement)
SCD-P08	<u>Community and Indigenous Data Consent</u> <i>CARE complements FAIR. People before data.</i>	GOVERNANCE	ILO Convention 169 — Indigenous and Tribal Peoples (ratified by Colombia, Peru, Bolivia, Mexico)
SCD-P09	<u>Regulatory Stack Alignment</u> <i>Build once, report everywhere.</i>	GOVERNANCE	EU Directive 2024/825 (EmpCo/Green Claims) — enforcement September 27, 2026
SCD-P10	<u>Resilience, Security and Data Governance</u> <i>Sovereign data that can be lost is not sovereign.</i>	GOVERNANCE	Climate Data Steering Committee — Common Carbon Credit Data Model (2024)

Technical Quality

- **SCD-P01 — Verifiability by Design:** If it cannot be checked, it does not count.
- **SCD-P02 — FAIR Data Standards:** Findable. Accessible. Interoperable. Reusable.
- **SCD-P03 — Full Provenance Traceability:** Without provenance, a number is a narrative.
- **SCD-P04 — Methodological Sovereignty:** You own your data only if you own your method.
- **SCD-P05 — Temporal Persistence and Baseline Integrity:** A result without a baseline is a claim without evidence.

Digital Sovereignty

- [SCD-P06 — AI-Legibility](#): If an AI agent cannot cite you, you do not exist.
- [SCD-P07 — Third-Party Anchoring](#): Your claim is only as strong as its external anchor.

Governance and Social Legitimacy

- [SCD-P08 — Community and Indigenous Data Consent](#): CARE complements FAIR. People before data.
- [SCD-P09 — Regulatory Stack Alignment](#): Build once, report everywhere.
- [SCD-P10 — Resilience, Security and Data Governance](#): Sovereign data that can be lost is not sovereign.

API Access

This wiki is accessible via the BookStack REST API. All pages are public and require no authentication to read.

```
# List all principles pages
```

```
GET https://wiki.cleantechhub.net/api/pages?filter[book_slug]=sovereign-climate-data
```

```
# Get a specific principle by slug
```

```
GET https://wiki.cleantechhub.net/api/pages?filter[slug]=verifiability-by-design
```

```
# Search across all principles
```

```
GET https://wiki.cleantechhub.net/api/search?query=CBAM+embedded+carbon
```

```
# Machine-readable JSON-LD principles index
```

```
GET https://wiki.cleantechhub.net/api/pages?filter[book_slug]=sovereign-climate-data&format=json
```

A static machine-readable version is also available at:

```
https://wiki.cleantechhub.net/data/principles.json
```

```
https://wiki.cleantechhub.net/data/principles_jsonld.json
```

How to Cite This Framework

Maintained by: CleantechHUB | **Contact:** gideon.blaauw@cleantechhub.net | **Licence:** CC-BY 4.0 | **Version:** 1.0.0 | **Updated:** 2026-05-26

? Related: Climate Data Governance Framework

The governance framework operationalises these principles into enforceable rules, credential-gated roles, and regulatory compliance mappings:

- [Climate Data Governance Framework](#) — 5 chapters covering constitutional layer, roles & permissions, decision rules, technical standards, and regulatory mappings (EUDR, CSRD, CBAM, ISSB S2, Article 6.4)
- [Community Sovereign Role](#) — operationalises Principle 8 (CARE/FPIC) with structural enforcement at database level
- [AI Agent Role](#) — operationalises Principle 6 (AI-Legibility) with delegated credentials and mandatory PROV-O trails
- [7-Layer Technical Standards Stack](#) — maps principles to W3C, ISO, UNTP, and CTH-original standards

Technical Quality

Principles 1–5: Verifiability, FAIR standards, provenance, methodology, and temporal persistence.

P01 — Verifiability by Design

SCD-P01 · Principle 1 of 10
Verifiability by Design
“If it cannot be checked, it does not count.”
Technical Layer

Definition

Every metric in a climate claim must be independently verifiable by any third party — including AI agents — without requiring permission, credentials, or manual intervention from the originating organisation. Verification must be possible from the primary source data alone.

Rationale

The EU Green Claims Directive (2024/825, enforcement September 2026) bans environmental claims that cannot be substantiated with publicly accessible evidence. AI audit tools already scan public data continuously; unverifiable claims are either invisible or automatically flagged as greenwashing. In 2026, verifiability is not a differentiator — it is the minimum floor for market credibility.

Implementation Steps

1. Map every reported metric to its primary data source (satellite, government dataset, sensor).
2. Ensure the source is publicly accessible without authentication.
3. Document the verification pathway: source ? method ? aggregation ? reported figure.
4. Test: ask an independent analyst to verify your top 5 climate claims using only public data.
5. Resolve any metric that cannot be independently verified before publication.

Compliance Checklist

	Criterion	What it means
?	Metric-to-source mapping exists	Every reported figure has a documented primary source.
?	Sources are publicly accessible	No login or permission required to access primary sources.

	Criterion	What it means
?	Verification pathway documented	Steps to reproduce any metric from scratch are written down.
?	AI scan performed	Climate TRACE / GFW / EDGAR check confirms the org is findable.

Regulatory References

- EU Directive 2024/825 (Green Claims / EmpCo) — Art. 5, 6
- IPCC AR6 Working Group III — Chapter 2 (Emissions Methodologies)
- ISSB IFRS S2 — Para. 63 (Disclosure verification)

Recommended Tools and Platforms

Climate TRACE Global Forest Watch EDGAR (EU JRC) Copernicus / ESA

Keywords

verifiability greenwashing EU Green Claims Directive AI audit ESG verification

Related Principles: [SCD-P02](#) · [SCD-P03](#) · [SCD-P07](#)
Document ID: SCD-P01 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Technical Quality |
Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P02 — FAIR Data Standards

SCD-P02 · Principle 2 of 10
FAIR Data Standards
“Findable. Accessible. Interoperable. Reusable.”
Technical Layer

Definition

Climate data must conform to FAIR principles: Findable (machine-readable metadata, persistent identifiers such as DOIs or stable URLs), Accessible (open API or public download, no authentication required), Interoperable (standard open formats: JSON-LD, GeoJSON, CSV, NetCDF), and Reusable (explicit open licence, fully documented provenance).

Rationale

FAIR compliance is a prerequisite for integration into global platforms (Climate TRACE, GFW, EDGAR) and for citation in ISSB S2 and EU CSRD disclosures. Data that is not FAIR cannot contribute to the AI-driven due-diligence economy. The 'From FAIR to FAIR²' framework (Frontiers, 2025) extends FAIR to also require machine-actionability — data that an AI agent can not only read but act upon.

Implementation Steps

1. Assign a persistent identifier (DOI or stable public URL) to every dataset.
2. Publish data in at least one open format: JSON, CSV, GeoJSON, or NetCDF.
3. Add schema.org or DataCatalog markup to all public data pages.
4. Declare a Creative Commons or equivalent open licence on every dataset.
5. Register datasets with a public catalogue (CKAN, DataCite, or national open data portal).

Compliance Checklist

	Criterion	What it means
?	Persistent identifiers assigned	Every dataset has a DOI or stable URL that will not change.
?	Open format export available	Data downloadable as JSON, CSV, or GeoJSON without login.

	Criterion	What it means
?	schema.org markup present	Dataset metadata is readable by Google Dataset Search and AI agents.
?	Licence declared	Explicit open licence (CC-BY 4.0 recommended) on every dataset.

Regulatory References

- FAIR Data Principles — Wilkinson et al., Scientific Data (2016)
- EU CSRD — Art. 8 Digital Tagging & Machine-Readable Reporting
- ISSB IFRS S2 — Appendix A (Definitions, data quality)

Recommended Tools and Platforms

schema.org DataCite CKAN Zenodo OpenAire

Keywords

FAIR principles open data interoperability schema.org machine-readable data catalogue

Related Principles: [SCD-P01](#) · [SCD-P06](#)
Document ID: SCD-P02 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Technical Quality |
Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P03 — Full Provenance Traceability

SCD-P03 · Principle 3 of 10
Full Provenance Traceability
“Without provenance, a number is a narrative.”
Technical Layer

Definition

The complete chain of custody — from raw sensor or satellite observation to reported metric — must be documented and auditable. Required provenance fields: instrument ID, satellite scene ID and overpass timestamp, calibration method and version, analyst name and organisation, processing software version, and all transformations applied including unit conversions and spatial aggregations.

Rationale

Carbon credit verification under Verra VM0042 (2026) and CBAM third-party verification (EU 2023/956) both require proof that figures derive from primary instruments, not secondary aggregations of uncertain origin. Digital MRV (dMRV) standards from the Planet2050 × BioCarbon Working Group (2025) identify broken provenance as the leading cause of carbon credit invalidation.

Implementation Steps

1. For each reported metric, create a provenance record with: source instrument, timestamp, analyst, methodology version, and transformations applied.
2. Store provenance records in a format that is exportable and machine-readable (JSON-LD recommended).
3. Link provenance records to the reported metric via persistent identifier.
4. Implement versioning: when methodology changes, create a new version record — never overwrite.
5. For satellite-derived data: record scene ID, sensor, orbit number, cloud cover, and NDVI delta.

Compliance Checklist

	Criterion	What it means
--	-----------	---------------

?	Instrument/source documented	Every metric traces to a named instrument or dataset version.
?	Timestamps recorded in UTC	All events use ISO 8601 UTC timestamps.
?	Analyst/author attributed	Name and organisation of every analyst is recorded.
?	Methodology version pinned	Specific version of methodology used is recorded, not just the name.

Regulatory References

- Verra VM0042 Methodology (2026 update) — Section 5 (MRV requirements)
- CBAM Regulation EU 2023/956 — Art. 10 (Embedded emissions calculation)
- dMRV Working Group — Planet2050 × BioCarbon (2025)

Recommended Tools and Platforms

ESA Sentinel-2 scene IDs NASA Landsat overpass metadata IDEAM Colombia GFW GLAD Lab

Keywords

provenance chain of custody MRV dMRV carbon verification Verra CBAM

Related Principles: [SCD-P01](#) · [SCD-P04](#) · [SCD-P05](#)
Document ID: SCD-P03 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Technical Quality |
Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P04 — Methodological Sovereignty

SCD-P04 · Principle 4 of 10
Methodological Sovereignty
“You own your data only if you own your method.”
Technical Layer

Definition

An organisation possesses genuine data sovereignty only if it also controls its methodology. Methodology must be: (a) documented in writing by the organisation, (b) aligned to a public standard (IPCC AR6, GRI 305, ISSB S2, Verra VM0042), and (c) reproducible by a qualified third party without reference to any vendor system. If the methodology belongs to a vendor, the organisation is 'controlled' at best.

Rationale

Vendors change pricing, pivot strategy, or cease operations. Organisations that outsource methodology without documentation lose all historical comparability overnight when a vendor changes its models. This is a form of retroactive data sovereignty collapse. The World Bank Sovereign Climate Reporting Framework (2022) and Cambridge Core Data & Policy Journal (2024) both identify methodology lock-in as the primary long-term risk in climate data infrastructure.

Implementation Steps

1. Write your own methodology document — not a reference to a vendor's documentation.
2. Anchor every calculation to a specific section of a public standard (e.g. IPCC AR6 WG3 §2.3).
3. Have the methodology reviewed by an independent expert at least once per year.
4. When vendors update their models, log the change and restate historical figures if material.
5. Store the methodology document in your own systems, not exclusively on a vendor platform.

Compliance Checklist

	Criterion	What it means
--	-----------	---------------

?	Own methodology document exists	A document you wrote describes how each metric is calculated.
?	Anchored to public standard	Each calculation references a specific section of IPCC AR6 / GRI / ISSB.
?	Independently reproducible	A qualified analyst could reproduce your results using only your document.
?	Vendor-change log maintained	Changes to vendor models that affect your figures are documented.

Regulatory References

- IPCC AR6 — Annex II (Methodologies for GHG inventories)
- GRI 305 (Emissions) — 2016, mandatory methodology disclosure
- World Bank — Sovereign Climate and Nature Reporting Framework (2022)

Recommended Tools and Platforms

GHG Protocol Corporate Standard IPCC Emission Factor Database (EFDB) GRI 305 reporting tool

Keywords

methodology sovereignty vendor lock-in GRI 305 IPCC AR6 carbon accounting reproducibility

Related Principles: [SCD-P03](#) · [SCD-P05](#)
Document ID: SCD-P04 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Technical Quality |
Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P05 — Temporal Persistence and Baseline Integrity

SCD-P05 · Principle 5 of 10
Temporal Persistence and Baseline Integrity
“A result without a baseline is a claim without evidence.”
Technical Layer

Definition

Sovereign climate data requires: (a) a documented, defensible baseline established before intervention begins; (b) historical data that is permanently owned and accessible regardless of vendor relationships; and (c) consistent methodology applied longitudinally — or, where methodology changes, an explicit reconciliation of the historical series to the new methodology.

Rationale

Investors and regulators need longitudinal data to assess whether impact is improving over time. A single-year snapshot without a consistent baseline is commercially and legally worthless for bond verification, carbon credit issuance, or ISSB S2 reporting. CEPAL's Sustainable Bonds LAC analysis (2024) found that the absence of defensible baselines is the primary reason LATAM green bonds cannot demonstrate impact at renewal.

Implementation Steps

1. Define and document your baseline before any intervention — not retroactively.
2. Store at least 3 years of historical data in systems you own and control.
3. When changing providers, negotiate full historical data export as a contractual condition.
4. Apply ISSB S2's transition provisions: restate comparatives when methodology changes.
5. Conduct an annual baseline review to confirm it remains defensible against current standards.

Compliance Checklist

	Criterion	What it means
?	Baseline documented pre-intervention	Baseline was set before the activity it measures, with date stamp.

	Criterion	What it means
?	3+ years of history owned	Historical data is in your own systems, not exclusively with a vendor.
?	Methodology consistent or reconciled	Any methodology changes are logged with impact on historical figures.
?	Annual baseline review conducted	Baseline reviewed annually against current IPCC / GRI standards.

Regulatory References

- ISSB IFRS S2 — Para. 22–28 (Transition provisions and comparatives)
- CEPAL — Sustainable Bonds LAC: Decade of Growth 2014–2024
- GRI 305-1 (Scope 1 GHG) — Section 3.3 (Base year recalculation policy)

Recommended Tools and Platforms

EDGAR time series GFW Hansen dataset v1.11+ IDEAM national GHG inventory series

Keywords

baseline temporal consistency historical data GHG inventory bond verification ISSB S2

Related Principles: [SCD-P04](#) · [SCD-P08](#)
Document ID: SCD-P05 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Technical Quality |
Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

Digital Sovereignty

Principles 6–7: AI-legibility and third-party anchoring.

P06 — AI-Legibility

SCD-P06 · Principle 6 of 10

AI-Legibility

“If an AI agent cannot cite you, you do not exist.”

Digital Layer

Definition

Climate data and impact claims must be structured so that AI agents can discover, parse, cite, and cross-reference them without human intermediation. Minimum requirements: schema.org/Dataset markup on all public pages, JSON-LD structured data, persistent canonical URLs, and inclusion in at least one major open index (Global Forest Watch, Climate TRACE, EDGAR, or Copernicus).

Rationale

The AI+ESG verification market is growing at 28% CAGR and already processes over 100,000 ESG sources daily using NLP models (WEF, 2024). AI agents are used by investors, regulators, and procurement teams for automated due diligence — without notifying the organisations being assessed. An organisation invisible to AI agents is invisible to the decision-makers those agents serve. Critically: AI without grounded sovereign data can also hallucinate plausible-sounding figures — making sovereign data not just a visibility tool but a truth anchor.

Implementation Steps

1. Add schema.org/Dataset JSON-LD to every public data page (see JSON-LD reference below).
2. Submit datasets to Google Dataset Search via schema.org markup.
3. Register with at least one global open data index (CKAN, DataCite, GFW API).
4. Maintain a public `llms.txt` file (analogous to `robots.txt`) guiding AI agents to authoritative sources.
5. Run quarterly AI scans: query Climate TRACE, GFW, and EDGAR to confirm your data is indexed.

JSON-LD Reference Example

```
{
  "@context": "https://schema.org",
  "@type": "Dataset",
  "name": "Colombia Deforestation Alerts 2024",
```

```
"description": "GLAD-L primary forest loss alerts for Colombia, 2024.",
"url": "https://data.cleantechhub.net/datasets/colombia-deforestation-2024",
"identifier": "https://doi.org/10.XXXX/cth-col-def-2024",
"creator": { "@type": "Organization", "name": "CleantechHUB" },
"datePublished": "2025-01-15",
"license": "https://creativecommons.org/licenses/by/4.0/",
"spatialCoverage": { "@type": "Place", "name": "Colombia" },
"temporalCoverage": "2024-01-01/2024-12-31",
"keywords": ["deforestation", "Colombia", "GLAD-L", "primary forest", "sovereign data"],
"distribution": [{
  "@type": "DataDownload",
  "encodingFormat": "application/json",
  "contentUrl": "https://data.cleantechhub.net/api/v1/datasets/colombia-deforestation-2024"
}]
}
```

Compliance Checklist

	Criterion	What it means
?	schema.org/Dataset markup live	JSON-LD is present on all public data pages and passes Google Rich Results test.
?	Listed in open index	Dataset appears in at least one: GFW API, Climate TRACE, EDGAR, DataCite.
?	llms.txt published	A public llms.txt file at cleantechhub.net/llms.txt guides AI agents.
?	Quarterly AI scan	Last scan date recorded; data confirmed indexed in at least one major platform.

Regulatory References

- EU CSRD — Art. 8 (machine-readable XBRL tagging requirement)
- TCFD Recommendations — Pillar 4 (Metrics and Targets, digital disclosure)
- IICSR AI+ESG Market Report 2025

Recommended Tools and Platforms

Google Rich Results Test schema.org validator llms.txt specification DataCite

Keywords

AI legibility schema.org JSON-LD ESG AI llms.txt due diligence NLP

Related Principles: [SCD-P01](#) · [SCD-P02](#)

Document ID: SCD-P06 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Digital Sovereignty |

Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P07 — Third-Party Anchoring

SCD-P07 · Principle 7 of 10
Third-Party Anchoring
“Your claim is only as strong as its external anchor.”
Digital Layer

Definition

Every sovereign climate claim must be anchored to at least one authoritative external source: a national government dataset (IDEAM, INPE/PRODES, SENAMHI, CONAF), a multilateral intergovernmental platform (GFW, Climate TRACE, EDGAR, Copernicus/ESA), or a certified third-party verifier accredited under an international standard (Verra, Gold Standard, CBAM-accredited VVB). Internal data alone, however well-documented, does not constitute sovereign climate data.

Rationale

Self-reported data without external anchor has zero credibility in investment due diligence, green bond verification, or regulatory audit. Anchoring to a sovereign or intergovernmental dataset transfers the burden of proof from the organisation to the global data infrastructure. For LATAM: IDEAM (Colombia), INPE/PRODES (Brazil), SENAMHI (Peru/Bolivia), and CONAF (Chile) are the authoritative national anchors for forest and climate data.

Implementation Steps

1. Identify the authoritative external source for each reported metric type (forest: GFW/IDEAM; emissions: Climate TRACE/EDGAR; energy: IEA/national grid operator).
2. Cross-reference your data against the external anchor at least quarterly.
3. Document discrepancies between your data and the anchor, with explanation.
4. For carbon credits: work only with verifiers accredited under Verra, Gold Standard, or a national carbon market standard.
5. For CBAM compliance: obtain third-party verification from an EU-accredited VVB.

Compliance Checklist

	Criterion	What it means
--	-----------	---------------

?	External anchor identified per metric	Each metric type has a named authoritative external source.
?	Quarterly cross-reference performed	Last reconciliation date recorded with discrepancy log.
?	Verifier accreditation confirmed	Any third-party verifier's accreditation status has been checked.
?	CBAM VVB in place (if applicable)	EU-accredited VVB identified for CBAM-relevant goods.

Regulatory References

- CBAM Regulation EU 2023/956 — Art. 10(3) (Accredited VVB requirement)
- Verra VCS Standard v4.1 — Section 4.2 (Validation and Verification)
- GFW GLAD-L Alert Methodology (Hansen et al. 2013, updated 2024)

Recommended Tools and Platforms

Global Forest Watch API Climate TRACE API EDGAR REST API Copernicus CDS API IDEAM Colombia INPE PRODES

Keywords

third-party verification IDEAM GFW EDGAR CBAM VVB carbon credits Verra

Related Principles: [SCD-P01](#) · [SCD-P03](#)
Document ID: SCD-P07 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Digital Sovereignty |
Source: CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

Governance and Social Legitimacy

Principles 8–10: Community consent, regulatory stack alignment, and resilience.

P08 — Community and Indigenous Data Consent

SCD-P08 · Principle 8 of 10

Community and Indigenous Data Consent

“CARE complements FAIR. People before data.”

Governance Layer

Definition

For climate data that touches territories, resources, or knowledge of indigenous or local communities — including forests, water, biodiversity, traditional ecological knowledge, and land-use data — the CARE Principles must complement FAIR: Collective Benefit (data use benefits the community, not just the collector), Authority to Control (communities control who accesses data about their territories), Responsibility (data users are accountable to the community), and Ethics (data collection, use, and sharing align with community values and rights). Free, Prior, and Informed Consent (FPIC) is required before data collection begins.

Rationale

In LATAM, most primary tropical forest is on indigenous or community land (Amazon, Andean communities, Mesoamerican forests, Pacific lowlands). Sovereign climate data built without community consent is: legally contested under ILO Convention 169 and national laws; technically incomplete (traditional ecological knowledge fills critical monitoring gaps); and ethically compromised. Post-COP15, the TNFD v1.0 framework — adopted by 320+ financial institutions — makes community rights a mandatory disclosure dimension. The Global Indigenous Data Alliance's CARE Principles (2019) are the operational framework; CODATA IDW 2025 reviewed their maturity model in practice.

Implementation Steps

1. Map all data collection activities against community land rights before beginning.
2. Obtain documented FPIC from affected communities before any data collection on their land.
3. Establish a data governance agreement that specifies community rights to access, correct, and withdraw consent for their data.
4. Ensure community members can access and challenge data about their territories.
5. Report on CARE compliance in the same place as FAIR compliance.

Compliance Checklist

	Criterion	What it means
?	Community land map completed	Data activities mapped against indigenous and community land rights.
?	FPIC documented	Free, Prior, and Informed Consent obtained and documented before data collection.
?	Data governance agreement signed	Agreement specifies community rights and responsibilities of the collector.
?	Community access enabled	Communities can view, challenge, and request correction of data about their land.

Regulatory References

- ILO Convention 169 — Indigenous and Tribal Peoples (ratified by Colombia, Peru, Bolivia, Mexico)
- TNFD Framework v1.0 (2023) — Core Disclosure B (Stakeholder engagement)
- Global Indigenous Data Alliance — CARE Principles for Indigenous Data Governance (2019)
- CBD Kunming-Montreal Framework (COP15, 2022) — Target 22 (Indigenous rights)

Recommended Tools and Platforms

RAISG Indigenous Territories Map
FAO FPIC Guidelines
CARE Data Maturity Model

Keywords

CARE principles indigenous data sovereignty FPIC community consent TNFD ILO 169 LATAM

Related Principles: [SCD-P09](#) · [SCD-P10](#)
Document ID: SCD-P08 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Governance and Social Legitimacy | **Source:** CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P09 — Regulatory Stack Alignment

SCD-P09 · Principle 9 of 10
Regulatory Stack Alignment
“Build once, report everywhere.”
Governance Layer

Definition

Sovereign climate data must be structured from inception to satisfy multiple simultaneous regulatory requirements without re-engineering. The 2026 regulatory stack includes: EU Green Claims Directive (enforcement September 2026), CBAM embedded carbon verification (fully operational January 2026), ISSB S2 mandatory disclosure (Brazil CVM, Mexico CNBV, Chile CMF — all from 2026), CSRD third-country scope (2029), Article 6 Paris Agreement carbon market rules (finalised COP29, 2025), and domestic NDC reporting requirements across LATAM.

Rationale

Organisations that build data infrastructure aligned to only one regulatory standard face costly rebuilds as additional mandates come into force. The 2026 stack creates immediate, simultaneous exposure across multiple jurisdictions for most LATAM organisations with international operations or finance. CBAM alone creates direct financial penalties — not just reputational risk — for LATAM exporters of steel, cement, aluminium, fertilizers, and hydrogen who cannot verify embedded carbon. Article 6 rules (COP29, Belém 2025) mean sovereign data is now a prerequisite for participating in international carbon markets.

Implementation Steps

1. Audit your regulatory exposure: which of the 2026 stack applies to your organisation?
2. Map each regulatory requirement to specific data fields (see Regulatory Mapping Table below).
3. Design data collection to capture all required fields from the start — not retrofit.
4. Use ISSB S2 as the baseline (it has the broadest adoption) and layer CBAM and GCD requirements on top.
5. Review the stack annually: add new requirements as they come into force.

Regulatory Mapping Table — 2026 Stack

Regulation	Jurisdiction	In Force	Key Data Requirement	Penalty
EU Green Claims Directive 2024/825	EU (affects global exporters)	Sept 2026	Substantiation of all environmental claims with verifiable evidence	Up to 4% annual turnover
CBAM (EU 2023/956)	EU imports — global exporters	Jan 2026 (full)	Embedded GHG per tonne for 6 product categories	Default tariff + penalties
ISSB IFRS S2	Brazil (CVM), Mexico (CNBV), Chile (CMF)	FY2025 data, reported 2026	Climate risks, Scope 1/2/3 emissions, scenario analysis	Securities regulator sanctions
EU CSRD	EU + large non-EU subsidiaries	2029 (third-country)	Full ESG disclosure per ESRS standards with XBRL tagging	EU market access risk
Paris Agreement Art. 6	LATAM sovereign govts	COP29 rules, 2025	Sovereign-grade MRV for internationally transferred mitigation outcomes (ITMOs)	Exclusion from international carbon markets

Compliance Checklist

	Criterion	What it means
?	Regulatory exposure audit completed	Applicable regulations from the 2026 stack identified.
?	Regulatory-to-data field mapping	Each regulation's key data requirements mapped to existing or planned fields.
?	ISSB S2 baseline in place	Data architecture covers all ISSB S2 mandatory disclosures.
?	CBAM readiness assessed	Embedded carbon calculation capability assessed for all relevant export products.

Regulatory References

- EU Directive 2024/825 (EmpCo/Green Claims) — enforcement September 27, 2026
- CBAM Regulation EU 2023/956 — definitive regime January 1, 2026
- ISSB IFRS S2 — S&P Global LATAM Adoption Map, June 2025
- Paris Agreement Article 6 — COP29 Rulebook (Belém, November 2025)

Recommended Tools and Platforms

Keywords

CBAM ISSB S2 EU Green Claims CSRD Article 6 COP29 regulatory compliance LATAM 2026

Related Principles: [SCD-P01](#) · [SCD-P02](#) · [SCD-P04](#)

Document ID: SCD-P09 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Governance and Social Legitimacy | **Source:** CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

P10 — Resilience, Security and Data Governance

SCD-P10 · Principle 10 of 10

Resilience, Security and Data Governance

“Sovereign data that can be lost is not sovereign.”

Governance Layer

Definition

Sovereign climate data requires an explicit governance framework specifying: (a) who has authority to read, write, modify, and delete data; (b) how data disputes are resolved; (c) backup and disaster recovery procedures; (d) security controls against unauthorised access or manipulation; (e) data retention and archiving policy; and (f) rules for data sharing with third parties. Governance must be documented and reviewed annually.

Rationale

Data sovereignty without governance is operational fiction. The Climate Data Steering Committee's Common Carbon Credit Data Model (2024) and the dMRV Working Group's Phase 2 Roadmap (2025) both identify data governance as the most under-addressed dimension of climate data infrastructure globally. For LATAM organisations, the additional risk is structural: most climate data is held in a single vendor system with no backup, no access log, and no recovery plan — meaning one vendor outage or relationship breakdown causes irreversible data loss.

Implementation Steps

1. Write a Data Governance Policy covering: access control (who can do what), dispute resolution, retention schedule, backup frequency, and sharing rules.
2. Implement role-based access: at minimum, separate read and write permissions.
3. Run automated backups to a system you control at least weekly; test recovery quarterly.
4. Maintain an access log: every read and write to sensitive climate data is recorded.
5. For shared data: use a Data Sharing Agreement (DSA) that specifies permitted uses, attribution requirements, and data return/destruction obligations.

Compliance Checklist

	Criterion	What it means
?	Data Governance Policy written	Document covers access control, disputes, retention, backup, and sharing.
?	Role-based access implemented	At minimum: separate read vs. write access for climate data systems.
?	Automated backups running	Weekly backup to a system you own, with quarterly recovery tests.
?	Access log active	All reads and writes to sensitive climate data are recorded with timestamp.

Regulatory References

- Climate Data Steering Committee — Common Carbon Credit Data Model (2024)
- dMRV Working Group Phase 2 Roadmap (Planet2050 × BioCarbon, 2025)
- GDPR Art. 5 (Data integrity and confidentiality) — applicable to EU-adjacent organisations
- ISO/IEC 27001 (Information Security Management) — international baseline

Recommended Tools and Platforms

Infisical (secrets management) Backblaze B2 / Rclone (backup) Keycloak (access control) Audit log frameworks

Keywords

data governance security resilience backup access control data sharing agreement ISO 27001

Related Principles: [SCD-P04](#) · [SCD-P08](#)
Document ID: SCD-P10 | **Version:** 1.0.0 | **Last Updated:** 2026-05-26 | **Category:** Governance and Social Legitimacy | **Source:** CleantechHUB Sovereign Climate Data Framework | **Licence:** CC-BY 4.0

This page is part of the [Sovereign Climate Data Wiki](#), maintained by CleantechHUB. It is AI-legible, machine-readable, and available via the [BookStack REST API](#).

API Reference

API Reference — Sovereign Climate Data Wiki

All pages in this book are publicly accessible via the BookStack REST API. No authentication is required for read access.

Base URL

`https://wiki.cleantechhub.net/api`

Common Queries

Purpose	Endpoint
List all principles pages	<code>GET /api/pages?filter[book_slug]=sovereign-climate-data</code>
Get a principle by slug	<code>GET /api/pages?filter[slug]=verifiability-by-design</code>
Get full page content	<code>GET /api/pages/{id}</code>
Search all principles	<code>GET /api/search?query=CBAM+embedded+carbon</code>
List chapters	<code>GET /api/chapters?filter[book_id]=860</code>
Get book metadata	<code>GET /api/books/860</code>

Static Machine-Readable Files

Format	URL	Use case
Flat JSON	<code>https://wiki.cleantechhub.net/data/principles.json</code>	General API consumers, dashboards
JSON-LD (schema.org)	<code>https://wiki.cleantechhub.net/data/principles_jsonld.json</code>	AI agents, Google Dataset Search, semantic web

Example: Fetch Principle P01 as JSON

```
curl -s "https://wiki.cleantechhub.net/api/pages?filter[slug]=verifiability-by-design" \
| python3 -c "import sys,json; d=json.load(sys.stdin); print(d['data'][0]['name'])"
```

Example: Search for CBAM-related principles

```
curl -s "https://wiki.cleantechhub.net/api/search?query=CBAM" \
| python3 -m json.tool | grep -A3 '"name"'
```

Example: Pull principles.json for RAG ingestion

```
import requests
data = requests.get("https://wiki.cleantechhub.net/data/principles.json").json()
for p in data["principles"]:
    print(p["id"], p["title"])
```

Rate Limits

BookStack imposes no rate limit on read-only API calls. Be courteous: add a 100ms delay between calls in scripts.

Licence

All content in this wiki is published under [CC-BY 4.0](#). Cite as: CleantechHUB (2026). *Sovereign Climate Data Principles*, v1.0.0.