Governance and Social Legitimacy

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

- P08 — Community and Indigenous Data Consent
- P09 — Regulatory Stack Alignment
- P10 — Resilience, Security and Data Governance

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

ISSB IFRS S2 disclosure checklist CBAM Registry EU CSRD ESRS standards LATAM NDC tracker (CEPAL)

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.