Data Safety Policy for Trade Unions and Civil Society Organizations

Updated January 22, 2026

The TU/CSO Data Safety Policy is implemented alongside Open Supply Hub's existing governance and accountability frameworks, including its Safeguarding Policy and Whistleblower Policy. Together, these policies establish complementary and reinforcing mechanisms for identifying risks, raising concerns, reporting harm, and seeking redress where appropriate.

I. Purpose

This policy outlines how Open Supply Hub (OS Hub) collaborates with trade unions (TUs) and civil society organizations (CSOs) when sharing supply chain data for inclusion in the OS Hub database.

It builds on OS Hub's 2025 report, *Beyond Transparency,* which captured key insights from TUs and CSOs on how digital supply chain accountability tools, such as OS Hub, should handle data from these actors, particularly in ways that ensure trust, safety, consent, and reciprocity.

This policy complements, but does not replace, OS Hub's Terms of Use and Data Use Policies. Data contributed by TUs and CSOs prior to this date may or may not have been reviewed under this process, whereas all future data contributions will follow this policy.

OS Hub will continue to refine and iterate this policy based on feedback. If you have comments or suggestions, you can share them through this feedback form.

II. Roles

Contributors (Trade Unions / Civil Society Organizations)

Contributors are the primary sources of the data they submit to OS Hub. They are responsible for ensuring that submissions are accurate, safe to share, and made with the necessary organizational consent. The final decision to contribute data rests entirely with the contributor.

Open Supply Hub (OS Hub)

OS Hub facilitates the process by:

- Providing risk guidance on potential safety, legal, and reputational risks through its staff and advisory committee;
- Applying the Safety Review Gate (see below) before publication to identify and mitigate possible harms; and
- Supporting contributors with feedback, anonymization options, and practical measures to minimize risk and enhance data quality.

Data Users

Data Users may access and use published data in accordance with OS Hub's Terms of Service.

Ownership & Licensing

All data published on OS Hub is shared under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. This means that contributors remain recognized as the source of their data, while OS Hub hosts, curates, and publishes it for open use consistent with this license.

III. Data Types & Consent

To ensure safety, OS Hub distinguishes between two main categories of data: organizational data and personal or sensitive data.

Organizational Data

Refers to information about institutions, workplaces, or collective structures, not individual persons.

Examples (some, not all):

- Factory or supplier lists by region
- Existence of collective bargaining agreements (CBAs) or grievance mechanisms
- Factories or workplaces covered in a research study
- Union or CSO-led initiatives, campaigns, or monitoring activities

Personal or Sensitive Data

Refers to information that could identify, expose, or endanger an individual.

Examples (some, not all):

- Names, contact details, or photographs of workers, labor organizers, or whistleblowers
- Individual case narratives or testimonies with identifiable details
- Any data that could be traced back to a person through their location, job title, or incident description

Policy: OS Hub does not accept personal or sensitive data for upload, as it cannot guarantee safety once such information becomes public.

Withdrawal Rights

Contributors may request the removal of their data at any time. Urgent requests (e.g., related to safety or legal threats) will be processed within two business days wherever possible.

Attribution

When it is safe to do so, OS Hub will credit the contributing organization by name.
If contributors prefer not to be named, the attribution will show that the entry has been contributed by *"A Civil Society Organization or A Union."*

IV. Safety Review Gate

Before any TU or CSO submission is published on OS Hub, it goes through a Safety Review Gate. This process helps identify and reduce risks to contributors, workers, and communities before data becomes publicly visible. Each submission is reviewed by both the OS Hub team and at least one member of the 'Advisory Committee on Trade Union & CSO Engagement', prior to publication.

Who Conducts the Review

The Advisory Committee is composed of individuals who work with, or have worked closely with, trade unions and civil society organizations, and who understand the political and civic risks faced in different regions.

All Advisory Committee members are expected to handle submissions with strict confidentiality and care. They review information only for the purpose of assessing potential safety, legal, or privacy risks, and are not permitted to share or discuss data outside the review process.

If the Advisory Committee determines that it lacks the sectoral or regional expertise needed for a particular submission, OS Hub may, in consultation with the committee and the submitting organization, invite a trusted external expert to support the review. Any external expert involved will also be required to follow the same confidentiality expectations and limited-use purpose.

To ensure transparency, contributors may request the name and details of the Advisory Committee member reviewing their submission. Contributors may also request a short clarification call with the reviewing member to discuss context or possible risk-mitigation options before a final decision is made.

Focus Areas of Review

At present, OS Hub's Safety Review Gate focuses on three categories of risk.
These categories may evolve over time to reflect new contexts and lessons learned.

a. Freedom of Association (FOA) & Civic Space Risks

Key questions include:

- Could publication expose workers, organizers, or unions to retaliation or harassment?
- Does the data relate to a context where union or CSO activity is criminalized or heavily restricted?

OS Hub does not currently evaluate whether a union or organization is "legitimate" or "yellow." Such judgments fall outside our present mandate. In the future, OS Hub may develop different categories or identifiers for different forms of trade unions and CSOs (e.g. through icons or markers on the platform) to help users distinguish different types of organizations.

b. Legal & Compliance Risks

Key questions include:

- Could the submission be challenged as defamatory, misleading, or inaccurate?
- Are there foreseeable risks of litigation, liability, or other legal action against OS Hub or contributors?

- Does publication risk breaching national laws or any existing data-sharing agreements?

c. Data Sensitivity & Privacy Risks

Key questions include:

- Does the submission include personal or identifiable information (even if names are removed)?
- Could individuals be re-identified through job titles, incidents, or geographic details?
- Could the data be misused for surveillance, doxxing, or intimidation?
- Does the data include descriptions of violence or harassment that could retraumatize survivors if made public?

Timelines

Under normal circumstances, OS Hub aims to complete the Safety Review Gate within 10 working days of receiving a complete submission. For urgent submissions, for example, when publication is time-sensitive or linked to an active campaign, OS Hub will make every effort to review and publish within 5 working days, subject to the availability of reviewers and risk conditions.

Limitations

These above categories and timelines do not capture every possible scenario. OS Hub applies them using the best available judgment of its multi-country staff, Advisory Committee, and experts. However, complete protection cannot be guaranteed, and contributors are encouraged to weigh potential risks carefully before submission.

Possible Outcomes from the Safety Review

Outcome	Description
Publish	Data is approved for inclusion on OS Hub. Protective measures, such as anonymization, or limited attribution, may be applied.
Defer	Publication of data is temporarily postponed, pending clarification from the contributor or additional safeguards.
Quarantine / Decline	In consultation with the submitting organization, the data may be withheld from publication if it is assessed as too risky to release safely. OS Hub will work with the contributor to explore possible options, such as redaction, anonymization, or delayed publication, and the data will be securely stored and re-evaluated later, if and when conditions improve.

Decision Authority & Transparency

The TU/CSO Advisory Committee has the final say on all safety-related decisions with regard to a dataset. The committee's role is to safeguard contributors and rightsholders, ensuring that no data is published if it could reasonably expose individuals or groups to harm, retaliation, or legal risk.

Safety-related decisions are made through a contextual assessment rather than a checklist-based or automatic threshold approach. An affirmative response to one or more risk questions does not, on its own, result in rejection of a submission. Instead, the committee considers whether identified risks can be reasonably mitigated through measures such as anonymization, redaction, delayed publication, limited attribution, or additional safeguards.

If the committee determines that a dataset or part of it poses an unmanageable risk, it will not be published until the risk can be mitigated. This decision reflects a shared commitment to "do no harm" and to prioritize safety over visibility.

Where a submission is deferred, modified, or declined on safety grounds, Advisory Committee members will be available to speak directly with the contributing organization to clarify concerns, explain the reasoning behind the decision, and explore alternative, safer ways to support or represent the data.

To support consistency, accountability, and institutional learning over time, Open Supply Hub maintains an internal record of Safety Review Gate decisions and related rationale. This record is used for governance and reference purposes, including as Advisory Committee membership evolves, and is not publicly accessible.

V. Redress, Correction & Takedown

OS Hub recognizes that circumstances, risks, or facts may change after data has been published on the platform. To uphold the principle of "*do no harm*," contributors and affected parties have pathways to request corrections, removals, or other forms of redress when necessary.

How to File a Request

Requests can be submitted by:

- The contributing trade union or civil society organization; or

- An authorized point of contact designated by the contributor.
  The name and contact details of the authorized representative should be provided at the time of data submission in OS Hub's official TU/CSO data submission form or via alternate pathways as agreed upon during the submission process.

Requests should be sent to support@opensupplyhub.org and may be written in any language. Submissions in local or regional languages will be translated internally where necessary to ensure timely and accurate follow-up.

Eligible Requests

OS Hub accepts redress, correction, or takedown requests for the following reasons (examples, not exhaustive):

- Safety threats: publication creates or increases a risk of harm, retaliation, or legal exposure.

- Inaccuracies or misattributions: factual errors, incorrect facility details, or wrong attribution.

- Consent withdrawal: the contributor or authorized representative withdraws permission to publish.

- Legal orders or restrictions: court orders, government directives, or other binding obligations.

- Other legitimate concerns: such as new contextual risks, privacy issues, or community-level appeals.

Available Actions

Depending on the nature of the request and the level of risk, OS Hub may:

- Temporarily hide the record while reviewing the issue;

- Correct or redact specific fields or text;

- Remove the record entirely from public view; or

- Add clarifying notes to provide verified updates or contextual explanations.

All actions are recorded in OS Hub's internal decision register to maintain accountability and consistency.

Timelines

- Urgent cases (for example, safety or legal threats) will be assessed and acted upon within two working days, wherever possible.

- Non-urgent cases will be reviewed within five working days. If a request arrives on a weekend or public holiday, processing will begin on the next working day.

Communication & Follow-up

Contributors will receive a notification once their request has been processed.
If further clarification is required, OS Hub staff or members of the Advisory Committee may reach out to discuss available options before finalizing an outcome.

Where a request highlights a broader or recurring pattern of risk, for example, repeated threats or region-specific restrictions, OS Hub may consult the Advisory Committee to ensure consistent treatment and collective learning across similar cases.

VI. Contributor Responsibilities

Trade unions (TUs) and civil society organizations (CSOs) that contribute data play a key role in ensuring that information shared through OS Hub remains credible, safe, and rights-respecting.
By submitting data, contributors agree to follow the principles below.

a. Do No Harm

Contributors should make every reasonable effort to ensure that publishing the data does not endanger workers, organizers, or communities. This includes conducting a basic risk scan before submission, consulting legal, digital-security, or organizational experts if needed.

b. Use Safe Channels

Data should be transferred only through safe and reliable channels. OS Hub accepts data through the official TU/CSO data submission form used for TU/CSO data submission. This form requires a Google log-in, which allows for secure transmission of files, according to Google policies. If, for any reason, this option is not comfortable or viable, OS Hub can work with contributors to identify alternative transfer methods that are appropriate to their context and risk level (for example, encrypted email or another mutually agreed channel).

c. Be Accurate and Fair

Provide the best-available and verifiable information at the time of submission.
If information is partial, under dispute, or awaiting confirmation, clearly mark it using qualifiers such as *"allegation," "pending verification,"* or *"approximate."*

d. Respect Consent

Before submitting, ensure that all relevant organizations or networks have consented to the inclusion of data about them. Personal or identifiable data should never be included.

e. Engage in Follow-Up

Contributors should remain available, where possible, to:

- Respond to OS Hub or Advisory Committee requests for clarification;

- Assist in identifying or resolving safety or accuracy issues that arise after publication.

f. Update or Withdraw When Needed

If any submitted information becomes outdated, inaccurate, or risky to keep online, contributors are encouraged to notify OS Hub promptly through the redress process (see below). This helps maintain accuracy and protects everyone involved.

VII. Policy Review

This policy will be reviewed at a minimum on an annual basis, and updated as needed to reflect legal, operational, or contextual changes affecting trade unions, civil society organizations, data contributors, or Open Supply Hub itself.

Any revisions will be versioned and published on Open Supply Hub's Governance & Policies page to ensure a single, authoritative reference point.

Annex A : Data Submission Form

Contributors can share organizational data with OS Hub using the following form:

OS Hub TU/CSO Data Submission Form: Please note that login to a Google account will be required to share data via this form. If you do not have a Google account and require an alternate method, please email support@opensupplyhub.org.

When submitting data, please include basic identifying information about each production location or workplace, for example:

- **Facility / Workplace Name**
- **Address (see guidance below)**
- **Sector/Industry**
- **Country**

Data may be submitted in any format (for example: spreadsheets, PDFs, short reports, or text files).

If you face challenges in using the Submission Form, such as limited connectivity, language barriers, or digital-security concerns, OS Hub can arrange alternative secure methods for submission, including Signal or encrypted email.

Guidance on Addresses

To ensure maximum accuracy and usability, addresses should follow the guidance below wherever possible:

Addresses should be complete and include:

- Street number
- Street name
- City or town

- Province or state

- Zip or postal code

If a street name and/or number is not available or does not exist, please use:

- Neighborhood name; and/or

- Village name; and/or

- Name of the industrial area and plot number(s); and/or

- Another locally recognized geographic identifier.

Additional guidance:

- Translate any non-Roman characters into their Roman / English equivalents.

- Remove Post Office Boxes or similar references (for example: P.O. Box, Caixa Postal, Apartado Postal), as these may interfere with geocoding and location accuracy.

If precise address details are difficult or risky to share, contributors are encouraged to flag this at the time of submission so that Open Supply Hub can explore appropriate safeguards during the Safety Review Gate.

Annex B – Takedown / Correction Request Template

To request a correction, redaction, or removal of data, please provide the following information.
You can copy this format into an email and send it to support@opensupplyhub.org in any language.

Subject line: Takedown / Correction Request

Requester name & role:

Record / URL / Facility identifier:
Identify the specific data-entry or dataset in question.

Issue type:
Please describe which issue applies, for example:

- Safety risk
- Inaccuracy
- Consent withdrawal
- Legal order (attach if available)

- Other (please explain)

Requested action:

Please specify what you would like OS Hub to do, for example:

- Redact specific details
- Hide temporarily
- Remove completely
- Other (please explain)

Reason & evidence:

Describe in no more than 500 words. Attach any supporting documents if available.

Preferred contact method:

(e.g., Signal, WhatsApp, email, or another safe channel)