



GoodWeave International

Data Sharing Protocol

Version 1, December 2016

Addendum to:
GWI Confidentiality Policy, November 2014

Contact for Comments:

info@goodweave.org

Next scheduled review:

December 2019

For further information:

<https://goodweave.org/policies-procedures/>

1. Background

As GoodWeave International (GWI) expands its mission of ending child labor beyond the carpet industry and into new sectors, it is important to establish organizational consistency on how data is collected and shared. With the advent of the Chainpoint web and mobile platforms, data is now accessible in real-time and larger quantities, with links to many stakeholders. The following is a set of guidelines to reference in cases when data sharing and data storage is required.

'Data sharing' can be defined as the disclosure or making known of quantitative and qualitative information, facts and statistics collected from one or more internal or external sources for reference or analysis between different parts of an organization or to a third party. Provisions for data sharing are not limited to personal data or raw data; it also includes aggregated organizational indicators, charts, audit information, etc. Data sharing is a natural component of organizational activity, and thus it is important to follow GWI's protocol and code of practice.

Data sharing and confidentiality go hand-in-hand, and both are critically important at GWI. GWI and its personnel have an ethical and legal obligation to respect the privacy and to protect and maintain the confidentiality of all information about companies (licensees, producers), workers, children and other program beneficiaries, their family members, and friends in the course of providing services to them as described in the GWI Confidentiality Policy. Every employee must read and agree to GWI's Confidentiality and Data Sharing Protocol Agreement (Appendix 1 to the Confidentiality Policy).

There are several categories of data sharing often referenced and covered under this protocol:

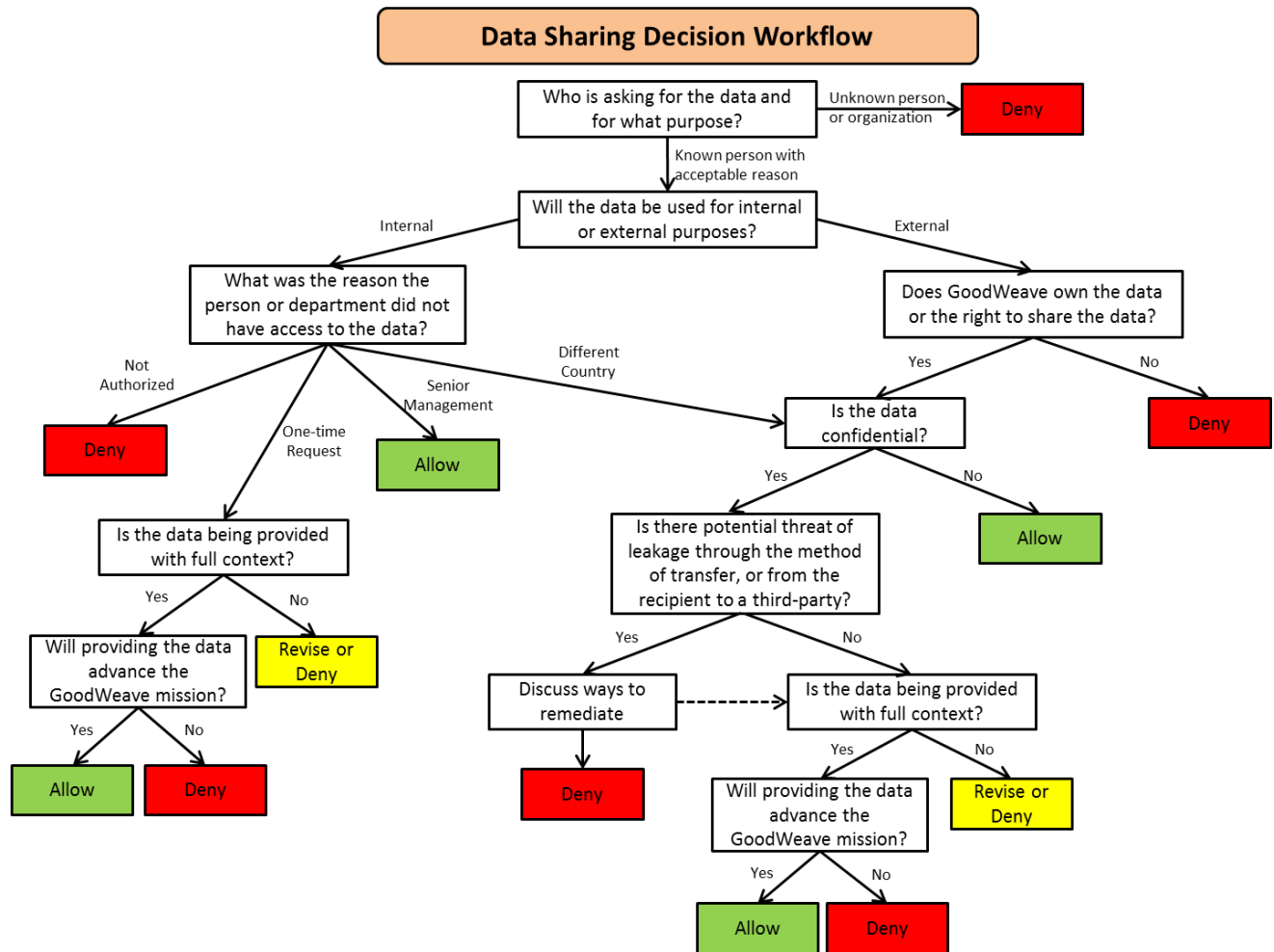
- Systematic data sharing: the routine sharing of data sets within or between organizations for an agreed purpose.
- Ad hoc data sharing: request to share data in a 'one-off' type of situation, which is not covered by any routine agreement. This may involve a decision about sharing being made in conditions of real urgency, or might be used to highlight a specific example.
- Sharing within the organization: sharing data which one may not have direct access to or transferring of data from a point-of-contact to other departments/members in the organization; particularly relevant for cross-country sharing.
- External reporting: sharing of data to external stakeholders, including donors and government officials.

2. Guidelines

In order to understand acceptable data sharing conditions the questions below should be used to help guide decision making.

- 1) Who is asking for the data and for what purpose?
- 2) Will the data be used for internal or external purposes?
- 3) What was the reason the person or organization did not have access to the data?
- 4) Does GoodWeave own the data or the right to share the data?
- 5) Is the data confidential? (see section 3 for additional guidelines)
- 6) Is the data being provided with full context?

- 7) Is there potential threat of leakage or accidental disclosure to another party through the method of information transfer, or from the recipient to a third party?
- 8) Will providing the data advance the GoodWeave mission?
- 9) What risk does the data sharing pose? (see 'data risk' under glossary of terms)
- 10) Does the party with whom you might share the data understand the GoodWeave data sharing protocol?
- 11) What information needs to be shared?



The questions above, and the decision workflow, have been established to provide a framework for how and when data sharing is appropriate. However, the above should not be used as an end-all solution to determining whether data sharing is appropriate or not. In the event of uncertainty, refrain from sharing data and contact your supervisor. If still uncertain, and the request is of high significance, the Executive Leadership Team (ELT) should be consulted.

3. Confidential versus Public Information

Public information generally refers to information that is already a matter of public record or knowledge. Confidential information is all other information which is not generally known to the

public and whose access is subject to restriction. The GWI Confidentiality Policy describes the distinction between public and confidential information further and provides examples of each.

Public information is not the primary focus of this Data Sharing Protocol. Particular attention should be paid to confidential data sharing such as (but not limited to) the following:

- Information related to the auditing, inspection and evaluation of licensees, their supply chains and parties applying for GoodWeave license/certification;
- Child labor and young worker non-compliances or specific information about children as further detailed in the GWI Child Protection Policy;
- Worker survey and worker interview data, collected via third party such as LaborLink, or by internal GoodWeave inspectors;
- Personnel files, including the staff, Board Members, Committee Members, contractors, and inspectors, including contact information, other than what is public information listed on the GoodWeave website;
- Information and data declared as “Confidential” by GWI personnel or under a non-disclosure agreement;
- Details of internal and external audits of GoodWeave’s certification program; or any other proprietary information.

If the result of a decision responding to a data sharing request is to share confidential data with an external party, a non-disclosure agreement (NDA) should be established before any such data is shared.

4. Programs and Stakeholders (Primary and Secondary)

Different categories of partners require different access to data. When initiating a new program, the primary and secondary stakeholders should be identified and appropriate types of data to be shared with each should be determined. The following are examples of some key programs and stakeholders for whom the data sharing protocol is relevant:

	Primary Stakeholders	Secondary Stakeholders
General operations	<ul style="list-style-type: none"> • GWI staff • GoodWeave country program/affiliate staff • Board of Directors • Certification Committee • Oversight Committee 	<ul style="list-style-type: none"> • Standards Committee • Program beneficiaries • Donors
Supply Unchained	<ul style="list-style-type: none"> • USAID • Skoll Foundation • Chainpoint • Target 	<ul style="list-style-type: none"> • Importers • Producers • Workers
Better Brick Nepal	<ul style="list-style-type: none"> • Humanity United • Global Fairness Initiative 	<ul style="list-style-type: none"> • Implementing Organizations • Kiln owners • Naikes • Workers • Nepal Government (including DCWB and police)

Apparel Pilot	<ul style="list-style-type: none"> • C&A Foundation • C&A Company 	<ul style="list-style-type: none"> • Producers(including Distribution Center owners/management) • Workers
---------------	---	---

5. User Types and User Roles in the Chainpoint Platform

The following are user roles as defined in the Chainpoint web platform. The reason for demarcation was to simplify the user-ability functions and control access to data specific to user needs. Lack of access does not necessarily imply mandatory control of data visibility among staff. For example, a country team auditor may need to see data relating to producers outside the scope of his/her entity access. However, the user should refer to the data sharing workflow in Section 2.

Role	Description
ChainPoint Administrator	<ul style="list-style-type: none"> • Has full access to all parts of the system and company data, until the end of the platform development.
GW administrator (Head office: 2-3 staff, most based in Washington DC, controlling authorizations of other users and global data)	<ul style="list-style-type: none"> • Has access to all non-coded parts of the system. • Can view all forms and access all reports and potentially access dashboards. • Has access to all company data, globally. • Has access to all used parts of administration. • Can add new companies and users.
GW staff (Head office staff, using platform for data and data analytics / reports)	<ul style="list-style-type: none"> • Can view all companies, supply chain data, audit reports, for all producer countries. • Can add/edit importer information (similar to Filemaker data interface).
GW country team administrator (Country office management and key personnel)	<ul style="list-style-type: none"> • Can add new users for specific country office. • Can do everything that country team staff can do (see below) • Has access to companies in the specified country/region(s).
GW report reviewer (Certification Division / Central Inspection Unit, including Director and admin support)	<ul style="list-style-type: none"> • Can do everything that country team staff can do (see below) • Can review, edit and approve or reject audit and inspection reports. • Has access to companies across countries/region(s).
GW country team staff (Field offices in Nepal, India and Afghanistan: could be inspectors, managers, admin staff, or social program staff)	<ul style="list-style-type: none"> • Can enter new producers, edit producer information & manage supplier relationships. • Can view all data relating to producers in the specified country/region. • Can schedule audits and assign to an auditor. • Can process label requests & issue invoices.

<p>GWI country team auditor (Limited to country inspectors)</p>	<ul style="list-style-type: none"> • Can conduct audits, inspections, CL/YW investigations, and worker interviews. • Have the ability to enter data using the mobile app or web platform. • Can view past audit reports, supply chain information for specified country/region & update supply chain links.
<p>Committee member (3-5 individuals based in North America, Europe, and Asia)</p>	<ul style="list-style-type: none"> • Can view producer, supply chain information, audit reports and selected dashboards (view only, not editing). • Can approve new licensee applicants (in future possibly also have the ability to approve/reject CARs, other decisions). • Restricted from viewing any invoicing/license fee data.
<p>External consultant</p>	<p>TBD</p>
<p>Licensed Importer (Approximately 140+ importers spread across North America, Europe, etc.)</p>	<p>TBD</p>
<p>Licensed Exporter (Approximately 170 total exporters spread across India, Nepal and Afghanistan)</p>	<p>TBD</p>

6. Other Considerations

Please refer to the GWI Confidentiality Policy for further information about conforming to information requests, confidentiality agreements, dealing with information/data sharing misconduct, and whistleblowing.

Glossary of terms¹

Anonymous Data: Any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely to be used to identify that individual.

Data: The physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means. Data may be numerical, descriptive or visual.

Data management: The development, execution and supervision of plans, policies and practices that govern data processing.

Data processing: Any operation or set of operations which is performed upon data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Data Risk:

- **High** risk data includes personal data, including any information that requires privacy and security protections, where data confidentiality is required by law, policy, or contractual obligations. It also includes data collected in programmatic, environmental, or political contexts where disclosure could cause direct harm to participants or put them at risk of adverse effects.
- **Medium** risk data includes business or strategic data, or any non-confidential internal data that should not be shared publicly, where unauthorized disclosure could cause material loss to the organization or brand risk. Includes aggregated data.
- **Low** risk data includes public data and data collected in low risk contexts, or information and programmatic, environmental, or political contexts where disclosure would not involve any risk to participants (would cause no adverse effect).

Informed consent: A process for getting willing permission to collect data of any kind based upon a clear appreciation and understanding of the facts, implications, and consequences of any engagement from participants.

Participants: A preferred term for data subjects, expanded to include any group, cooperative, or other entity with which GoodWeave works that provide program data.

Personal data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

¹ Adopted from Oxfam Responsible Program Data Policy; February 17, 2015