GRI STANDARDS

GRI GSSB

GRI 418: CUSTOMER PRIVACY
2016

GRI
418

Contents

About this Standard

Responsibility	This Standard is issued by the Global Sustainability Standards Board (GSSB). Any feedback on the GRI Standards can be submitted to standards@globalreporting.org for the consideration of the GSSB.
Scope	*GRI 418: Customer Privacy* sets out reporting requirements on the topic of customer privacy. This Standard can be used by an organization of any size, type, sector or geographic location that wants to report on its impacts related to this topic.
Normative references	This Standard is to be used together with the most recent versions of the following documents. *GRI 101: Foundation* *GRI 103: Management Approach* *GRI Standards Glossary* In the text of this Standard, terms defined in the Glossary are underlined.
Effective date	This Standard is effective for reports or other materials published on or after 1 July 2018. Earlier adoption is encouraged.

Note: This document includes hyperlinks to other Standards. In most browsers, using **'ctrl' + click** will open external links in a new browser window. After clicking on a link, use **'alt' + left arrow** to return to the previous view.

Introduction

A. Overview

This Standard is part of the set of GRI Sustainability Reporting Standards (GRI Standards). These Standards are designed to be used by organizations to report about their impacts on the economy, the environment, and society.

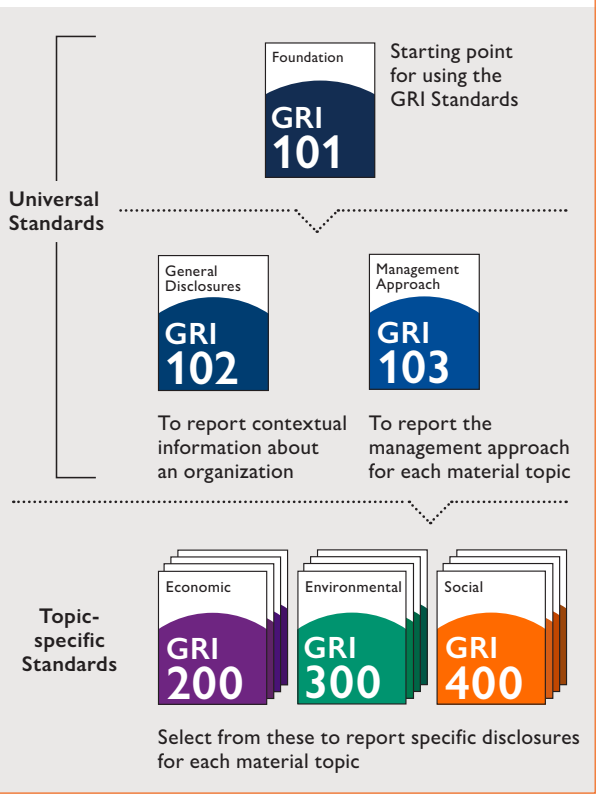
The GRI Standards are structured as a set of interrelated, modular standards. The full set can be downloaded at www.globalreporting.org/standards/.

There are three universal Standards that apply to every organization preparing a sustainability report:

GRI 101: Foundation
GRI 102: General Disclosures
GRI 103: Management Approach

***GRI 101: Foundation* is the starting point for using the GRI Standards. It has essential information on how to use and reference the Standards.**

Figure 1
Overview of the set of GRI Standards



An organization then selects from the set of topic-specific GRI Standards for reporting on its material topics. These Standards are organized into three series: 200 (Economic topics), 300 (Environmental topics) and 400 (Social topics).

Each topic Standard includes disclosures specific to that topic, and is designed to be used together with *GRI 103: Management Approach*, which is used to report the management approach for the topic.

***GRI 418: Customer Privacy* is a topic-specific GRI Standard in the 400 series (Social topics).**

B. Using the GRI Standards and making claims

There are two basic approaches for using the GRI Standards. For each way of using the Standards there is a corresponding claim, or statement of use, which an organization is required to include in any published materials.

1. The GRI Standards can be used as a set to prepare a sustainability report that is in accordance with the Standards. There are two options for preparing a report in accordance (Core or Comprehensive), depending on the extent of disclosures included in the report.

   An organization preparing a report in accordance with the GRI Standards uses this Standard, *GRI 418: Customer Privacy*, if this is one of its material topics.

2. Selected GRI Standards, or parts of their content, can also be used to report specific information, without preparing a report in accordance with the Standards. Any published materials that use the GRI Standards in this way are to include a 'GRI-referenced' claim.

See Section 3 of *GRI 101: Foundation* for more information on how to use the GRI Standards, and the specific claims that organizations are required to include in any published materials.

C. Requirements, recommendations and guidance

The GRI Standards include:

Requirements. These are mandatory instructions. In the text, requirements are presented in **bold font** and indicated with the word 'shall'. Requirements are to be read in the context of recommendations and guidance; however, an organization is not required to comply with recommendations or guidance in order to claim that a report has been prepared in accordance with the Standards.

Recommendations. These are cases where a particular course of action is encouraged, but not required. In the text, the word 'should' indicates a recommendation.

Guidance. These sections include background information, explanations and examples to help organizations better understand the requirements.

An organization is required to comply with all applicable requirements in order to claim that its report has been prepared in accordance with the GRI Standards. See *GRI 101: Foundation* for more information.

D. Background context

In the context of the GRI Standards, the social dimension of sustainability concerns an organization's impacts on the social systems within which it operates.

GRI 418 addresses the topic of customer privacy, including losses of customer data and breaches of customer privacy. These can result from non-compliance with existing laws, regulations and/or other voluntary standards regarding the protection of customer privacy.

These concepts are covered in key instruments of the Organisation for Economic Co-operation and Development: see References.

The disclosures in this Standard can provide information about an organization's impacts related to customer privacy, and how it manages them.

GRI 418: Customer Privacy

This Standard includes disclosures on the management approach and topic-specific disclosures. These are set out in the Standard as follows:

- Management approach disclosures (this section references *GRI 103)*
- Disclosure 418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data

1. Management approach disclosures

Management approach disclosures are a narrative explanation of how an organization manages a material topic, the associated impacts, and stakeholders' reasonable expectations and interests. Any organization that claims its report has been prepared in accordance with the GRI Standards is required to report on its management approach for every material topic, as well as reporting topic-specific disclosures for those topics.

Therefore, this topic-specific Standard is designed to be used together with *GRI 103: Management Approach* in order to provide full disclosure of the organization's impacts. *GRI 103* specifies how to report on the management approach and what information to provide.

Reporting requirements

1.1 The reporting organization shall report its management approach for customer privacy using *GRI 103: Management Approach*.

2. Topic-specific disclosures

Disclosure 418-1
Substantiated complaints concerning breaches of customer privacy and losses of customer data

Reporting requirements

Disclosure 418-1

The reporting organization shall report the following information:

a. Total number of substantiated complaints received concerning breaches of customer privacy, categorized by:

i. complaints received from outside parties and substantiated by the organization;

ii. complaints from regulatory bodies.

b. Total number of identified leaks, thefts, or losses of customer data.

c. If the organization has not identified any substantiated complaints, a brief statement of this fact is sufficient.

2.1 When compiling the information specified in Disclosure 418-1, the reporting organization shall indicate if a substantial number of these breaches relate to events in preceding years.

Guidance

Background

Protection of customer privacy is a generally recognized goal in national regulations and organizational policies. As set out in the Organisation for Economic Co-operation and Development (OECD) *OECD Guidelines for Multinational Enterprises*, organizations are expected to 'respect consumer privacy and take reasonable measures to ensure the security of personal data that they collect, store, process or disseminate'.

To protect customer privacy, an organization is expected to limit its collection of personal data, to collect data by lawful means, and to be transparent about how data are gathered, used, and secured. The organization is also expected to not disclose or use personal customer information for any purposes other than those agreed upon, and to communicate any changes in data protection policies or measures to customers directly.

This disclosure provides an evaluation of the success of management systems and procedures relating to customer privacy protection.

Glossary

This Glossary includes definitions for terms used in this Standard, which apply when using this Standard. These definitions may contain terms that are further defined in the complete *GRI Standards Glossary*.

All defined terms are underlined. If a term is not defined in this Glossary or in the complete *GRI Standards Glossary*, definitions that are commonly used and understood apply.

breach of customer privacy

non-compliance with existing legal regulations and (voluntary) standards regarding the protection of customer privacy

customer privacy

right of the customer to privacy and personal refuge

Note 1: Customer privacy includes matters such as the protection of data; the use of information or data for their original intended purpose only, unless specifically agreed otherwise; the obligation to observe confidentiality; and the protection of information or data from misuse or theft.

Note 2: Customers are understood to include end-customers (consumers) as well as business-to-business customers.

impact

In the GRI Standards, unless otherwise stated, 'impact' refers to the effect an organization has on the economy, the environment, and/or society, which in turn can indicate its contribution (positive or negative) to sustainable development.

Note 1: In the GRI Standards, the term 'impact' can refer to positive, negative, actual, potential, direct, indirect, short-term, long-term, intended, or unintended impacts.

Note 2: Impacts on the economy, environment, and/or society can also be related to consequences for the organization itself. For example, an impact on the economy, environment, and/or society can lead to consequences for the organization's business model, reputation, or ability to achieve its objectives.

material topic

topic that reflects a reporting organization's significant economic, environmental and social impacts; or that substantively influences the assessments and decisions of stakeholders

Note 1: For more information on identifying a material topic, see the Reporting Principles for defining report content in *GRI 101: Foundation*.

Note 2: To prepare a report in accordance with the GRI Standards, an organization is required to report on its material topics.

Note 3: Material topics can include, but are not limited to, the topics covered by the GRI Standards in the 200, 300, and 400 series.

substantiated complaint

written statement by regulatory or similar official body addressed to the organization that identifies breaches of customer privacy, or a complaint lodged with the organization that has been recognized as legitimate by the organization

References

The following documents informed the development of this Standard and can be helpful for understanding and applying it.

Authoritative intergovernmental instruments:

1. Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines for Multinational Enterprises*, 2011.

GRI STANDARDS

GRI GSSB

Legal liability

This document, designed to promote sustainability reporting, has been developed by the Global Sustainability Standards Board (GSSB) through a unique multi-stakeholder consultative process involving representatives from organizations and report information users from around the world. While the GRI Board of Directors and GSSB encourage use of the GRI Sustainability Reporting Standards (GRI Standards) and related Interpretations by all organizations, the preparation and publication of reports based fully or partially on the GRI Standards and related Interpretations are the full responsibility of those producing them. Neither the GRI Board of Directors, GSSB nor Stichting Global Reporting Initiative (GRI) can assume responsibility for any consequences or damages resulting directly or indirectly from the use of the GRI Standards and related Interpretations in the preparation of reports, or the use of reports based on the GRI Standards and related Interpretations.

Copyright and trademark notice

ISBN: 978-90-8866-129-7

standards@globalreporting.org
www.globalreporting.org

GRI
PO Box 10039
1001 EA
Amsterdam
The Netherlands