GRI STANDARDS

GRI 418: Customer Privacy 2016

EFFECTIVE DATE: 1 JULY 2018

TOPIC STANDARD

418

GRI 418: Customer Privacy 2016

Topic Standard

Effective date
This Standard is effective for reports or other materials published on or after 1 July 2018.

Responsibility
This Standard is issued by the Global Sustainability Standards Board (GSSB). Any feedback on the GRI Standards can be submitted to gssbsecretariat@globalreporting.org for the consideration of the GSSB.

Due Process
This Standard was developed in the public interest and in accordance with the requirements of the GSSB Due Process Protocol. It has been developed using multi-stakeholder expertise, and with regard to authoritative intergovernmental instruments and widely held expectations of organizations relating to social, environmental, and economic responsibilities.

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 the 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.

ISBN 978-90-8866-129-7

Contents

Introduction

GRI 418: Customer Privacy 2016 contains disclosures for organizations to report information about their impacts related to customer privacy, and how they manage these impacts.

The Standard is structured as follows:

- Section 1 contains a requirement, which provides information about how the organization manages its customer privacy-related impacts.
- Section 2 contains one disclosure, which provides information about the organization's customer privacy-related impacts.
- The Glossary contains defined terms with a specific meaning when used in the GRI Standards. The terms are underlined in the text of the GRI Standards and linked to the definitions.
- The Bibliography lists authoritative intergovernmental instruments used in developing this Standard.

The rest of the Introduction section provides a background on the topic, an overview of the system of GRI Standards and further information on using this Standard.

Background on the topic

This Standard 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 the Bibliography.

System of GRI Standards

This Standard is part of the GRI Sustainability Reporting Standards (GRI Standards). The GRI Standards enable an organization to report information about its most significant impacts on the economy, environment, and people, including impacts on their human rights, and how it manages these impacts.

The GRI Standards are structured as a system of interrelated standards that are organized into three series: GRI Universal Standards, GRI Sector Standards, and GRI Topic Standards (see Figure 1 in this Standard).

Universal Standards: GRI 1, GRI 2 and GRI 3

GRI 1: Foundation 2021 specifies the requirements that the organization must comply with to report in accordance with the GRI Standards. The organization begins using the GRI Standards by consulting *GRI 1*.

GRI 2: General Disclosures 2021 contains disclosures that the organization uses to provide information about its reporting practices and other organizational details, such as its activities, governance, and policies.

GRI 3: Material Topics 2021 provides guidance on how to determine material topics. It also contains disclosures that the organization uses to report information about its process of determining material topics, its list of material topics, and how it manages each topic.

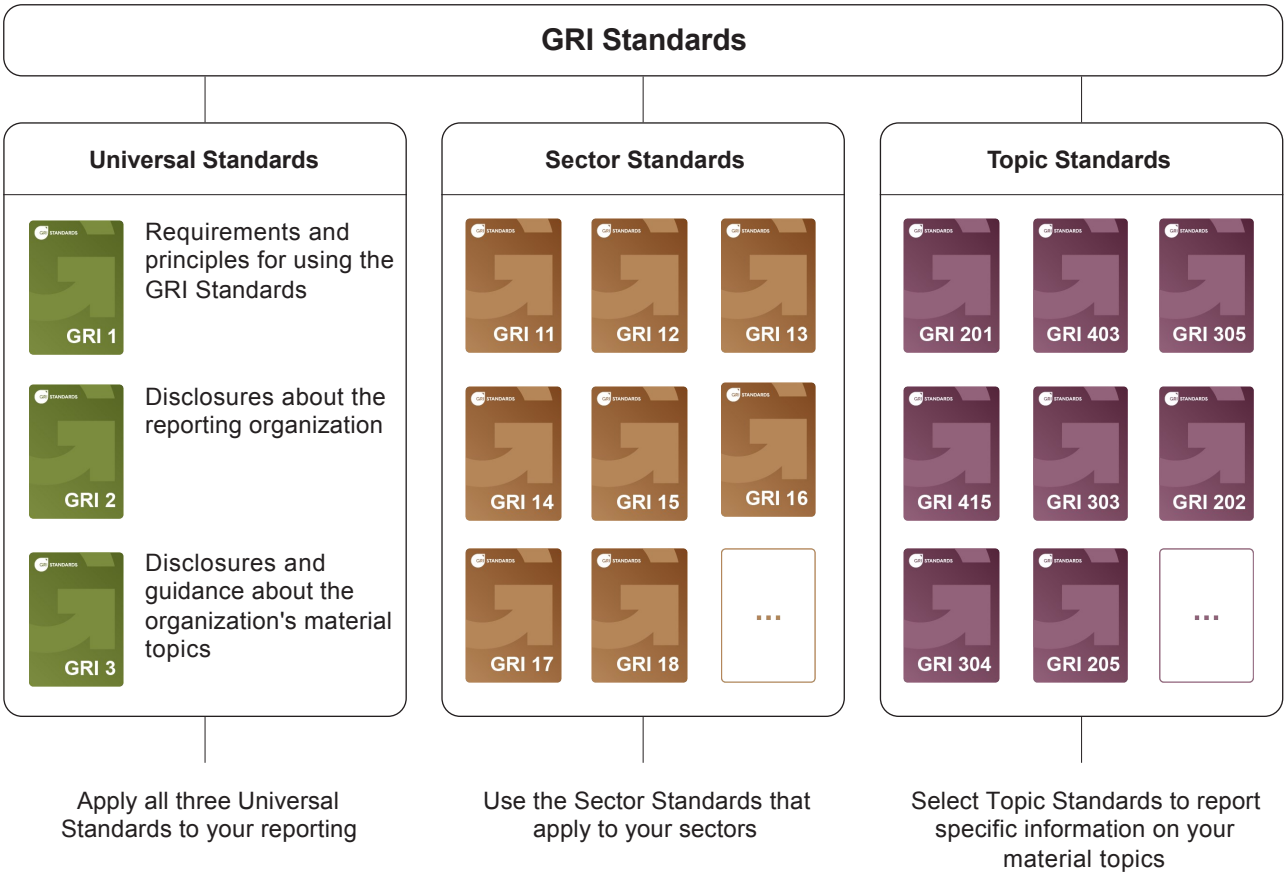
Sector Standards

The Sector Standards provide information for organizations about their likely material topics. The organization uses the Sector Standards that apply to its sectors when determining its material topics and when determining what to report for each material topic.

Topic Standards

The Topic Standards contain disclosures that the organization uses to report information about its impacts in relation to particular topics. The organization uses the Topic Standards according to the list of material topics it has determined using *GRI 3*.

Figure 1. GRI Standards: Universal, Sector and Topic Standards



Using this Standard

This Standard can be used by any organization – regardless of size, type, sector, geographic location, or reporting experience – to report information about its impacts related to customer privacy.

An organization reporting in accordance with the GRI Standards is required to report the following disclosures if it has determined customer privacy to be a material topic:

- Disclosure 3-3 in *GRI 3: Material Topics 2021* (see clause 1.1 in this Standard);
- Any disclosure from this Topic Standard that is relevant to the organization's customer privacy-related impacts (Disclosure 418-1).

See Requirements 4 and 5 in *GRI 1: Foundation 2021*.

Reasons for omission are permitted for these disclosures.

If the organization cannot comply with a disclosure or with a requirement in a disclosure (e.g., because the required information is confidential or subject to legal prohibitions), the organization is required to specify the disclosure or the requirement it cannot comply with, and provide a reason for omission together with an explanation in the GRI content index. See Requirement 6 in *GRI 1: Foundation 2021* for more information on reasons for omission.

If the organization cannot report the required information about an item specified in a disclosure because the item (e.g., committee, policy, practice, process) does not exist, it can comply with the requirement by reporting this to be the case. The organization can explain the reasons for not having this item, or describe any plans to develop it. The disclosure does not require the organization to implement the item (e.g., developing a policy), but to report that the item does not exist.

If the organization intends to publish a standalone sustainability report, it does not need to repeat information that it has already reported publicly elsewhere, such as on web pages or in its annual report. In such a case, the organization can report a required disclosure by providing a reference in the GRI content index as to where this information can be found (e.g., by providing a link to the web page or citing the page in the annual report where the information has been published).

Requirements, guidance and defined terms
The following apply throughout this Standard:

Requirements are presented in **bold font** and indicated by the word 'shall'. An organization must comply with requirements to report in accordance with the GRI Standards.

Requirements may be accompanied by guidance.

Guidance includes background information, explanations, and examples to help the organization better understand the requirements. The organization is not required to comply with guidance.

The Standards may also include recommendations. These are cases where a particular course of action is encouraged but not required.

The word ‘should’ indicates a recommendation, and the word ‘can’ indicates a possibility or option.

Defined terms are underlined in the text of the GRI Standards and linked to their definitions in the Glossary. The organization is required to apply the definitions in the Glossary.

1. Topic management disclosures

An organization reporting in accordance with the GRI Standards is required to report how it manages each of its material topics.

An organization that has determined customer privacy to be a material topic is required to report how it manages the topic using Disclosure 3-3 in *GRI 3: Material Topics 2021* (see clause 1.1 in this section).

This section is therefore designed to supplement – and not replace – Disclosure 3-3 in *GRI 3*.

REQUIREMENTS

1.1 The reporting organization shall report how it manages customer privacy using Disclosure 3-3 in *GRI 3: Material Topics 2021*.

2. Topic disclosures

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

REQUIREMENTS

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.

Compilation requirements

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 provides definitions for terms used in this Standard. The organization is required to apply these definitions when using the GRI Standards.

The definitions included in this glossary 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.

B

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

C

customer privacy
right of the customer to privacy and personal refuge

Examples: the obligation to observe confidentiality; the protection of data; the protection of information or data from misuse or theft; the use of information or data for their original intended purpose only, unless specifically agreed otherwise

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

H

human rights
rights inherent to all human beings, which include, at a minimum, the rights set out in the *United Nations (UN) International Bill of Human Rights* and the principles concerning fundamental rights set out in the *International Labour Organization (ILO) Declaration on Fundamental Principles and Rights at Work*

Source: United Nations (UN), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011; modified

Note: See Guidance to 2-23-b-i in *GRI 2: General Disclosures 2021* for more information on 'human rights'.

I

impact
effect the organization has or could have on the economy, environment, and people, including on their human rights, which in turn can indicate its contribution (negative or positive) to sustainable development

Note 1: Impacts can be actual or potential, negative or positive, short-term or long-term, intended or unintended, and reversible or irreversible.

Note 2: See section 2.1 in *GRI 1: Foundation 2021* for more information on 'impact'.

M

material topics
topics that represent the organization's most significant impacts on the economy, environment, and people, including impacts on their human rights

Note: See section 2.2 in *GRI 1: Foundation 2021* and section 1 in *GRI 3: Material Topics 2021* for more information on 'material topics'.

S

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

sustainable development / sustainability
development that meets the needs of the present without compromising the ability of future generations to meet their own needs

Source: World Commission on Environment and Development, *Our Common Future*, 1987

Note: The terms ‘sustainability’ and ‘sustainable development’ are used interchangeably in the GRI Standards.

Bibliography

This section lists authoritative intergovernmental instruments used in developing this Standard.

Authoritative instrument:

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

PO Box 10039
1001 EA Amsterdam
The Netherlands

www.globalreporting.org