

# GRI 418: Privacy dei clienti 2016

DATA DI ENTRATA IN VIGORE: 1 LUGLIO 2018

STANDARD SPECIFICO

# 418

# GRI 418: Privacy dei clienti 2016

## Standard specifico

### Data di entrata in vigore

Il presente Standard è in vigore per i report o altri materiali pubblicati a partire dal 1 luglio 2018.

### Responsabilità

Il presente Standard è emesso dal [Global Sustainability Standards Board \(GSSB\)](#). Eventuali riscontri sui GRI Standards possono essere inviati all'indirizzo [gssbsecretariat@globalreporting.org](mailto:gssbsecretariat@globalreporting.org) perché siano presi in considerazione dal GSSB.

### Iter procedurale

Il presente Standard è stato sviluppato nel pubblico interesse e in conformità ai requisiti del GSSB Due Process Protocol. È stato sviluppato utilizzando le competenze di vari stakeholder e tenendo presenti le autorevoli disposizioni di enti intergovernativi e aspettative diffuse di molteplici organismi – imprese commerciali, organizzazioni sindacali, società di investimento, istituti di mediazione e altri ancora – riguardanti responsabilità sociali, ambientali ed economiche.

### Responsabilità legale

Il presente documento, progettato per promuovere la rendicontazione di sostenibilità, è stato sviluppato dal Global Sustainability Standards Board (GSSB) attraverso un processo consultivo multistakeholder unico che ha coinvolto rappresentanti di organizzazioni e utilizzatori delle informazioni contenute nei report, provenienti da tutto il mondo. Sebbene il Consiglio di amministrazione di GRI e il GSSB incoraggino l'uso degli standard di rendicontazione di sostenibilità GRI (Standard GRI) e interpretazioni correlate da parte di molteplici organismi – imprese commerciali, organizzazioni sindacali, società di investimento, istituti di mediazione e altri ancora – la responsabilità della preparazione e pubblicazione di report basati, in tutto o in parte, sugli Standard GRI e interpretazioni correlate fa capo agli organismi che li redigono. Né il Consiglio di amministrazione del GRI né il GSSB né la fondazione Global Reporting Initiative (GRI) si assumono la responsabilità di qualsiasi conseguenza o danno risultanti, direttamente o indirettamente, dall'uso degli Standard GRI e interpretazioni correlate nella preparazione di report o nell'uso di report basati sugli Standard GRI e interpretazioni correlate.

### Copyright e marchio commerciale

Il presente documento è protetto da copyright detenuto dalla Fondazione Global Reporting Initiative (GRI). La riproduzione e distribuzione di questo documento a scopo informativo e/o l'uso per la preparazione di una rendicontazione di sostenibilità sono permesse senza previa autorizzazione del GRI. Tuttavia, né il presente documento né un qualsiasi suo estratto può essere riprodotto, archiviato, tradotto o trasferito in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, per fotocopie, registrazioni o altro) per qualsiasi altro scopo senza previa autorizzazione scritta del GRI.

Global Reporting Initiative, GRI e il logo, GSSB e il logo, e GRI Sustainability Reporting Standards (GRI Standards) e il logo sono marchi registrati della Fondazione Global Reporting Initiative.

# Indice

<b>Introduzione</b>	<b>4</b>
<b>1. Informative sulla gestione del tema</b>	<b>7</b>
<b>2. Informative sul tema</b>	<b>8</b>
Informativa 418-1 Denunce comprovate riguardanti le violazioni della privacy dei clienti e perdita di dati dei clienti	<b>8</b>
<b>Glossario</b>	<b>9</b>
<b>Bibliografia</b>	<b>11</b>

# Introduzione

*GRI 418: Privacy dei clienti 2016* contiene informative per le organizzazioni che devono rendicontare riguardo ai loro impatti correlati alla privacy dei clienti e sul modo in cui li gestiscono.

Lo Standard è strutturato come segue:

- La [Sezione 1](#) contiene un requisito, che fornisce informazioni su come l'organizzazione gestisce i propri impatti correlati alla privacy dei clienti.
- La [Sezione 2](#) contiene un'informativa, che fornisce informazioni sugli impatti dell'organizzazione correlati alla privacy dei clienti.
- Il [Glossario](#) contiene termini definiti con un particolare significato quando utilizzati negli Standard GRI. Tali termini sono sottolineati nel testo degli Standard GRI e collegati ipertestualmente alle loro definizioni.
- La [Bibliografia](#) elenca autorevoli strumenti di enti intergovernativi utilizzati per la preparazione del presente Standard.

Il resto della sezione Introduzione fornisce informazioni generali (background) sul tema, una descrizione generale del sistema degli Standard GRI e ulteriori informazioni sull'uso del presente Standard.

## Informazioni generali sul tema

Questo Standard tratta il tema della privacy dei clienti, in particolare la perdita di dati dei clienti e violazioni della loro privacy. Ciò può accadere per non conformità a leggi e regolamenti vigenti e/o ad altri standard volontari riguardanti la tutela della privacy dei clienti.

Questi concetti sono trattati in strumenti chiave dell'Organizzazione per la cooperazione e lo sviluppo economico; vedere la [Bibliografia](#).

## Sistema degli Standard GRI

Il presente Standard fa parte degli standard sulla rendicontazione di sostenibilità GRI (Standard GRI), che consentono a un'organizzazione di rendicontare informazioni relative ai suoi impatti più significativi sull'economia, sull'ambiente e sulle persone, inclusi quelli sui diritti umani, e a come gestisce tali impatti.

Gli Standard GRI sono strutturati come una serie di standard correlati tra loro, organizzati in tre serie: Standard GRI universali, Standard GRI di settore e Standard GRI specifici (vedere la [Figura 1](#) nel presente Standard).

### Standard universali: GRI 1, GRI 2 e GRI 3

[GRI 1: Principi di rendicontazione 2021](#) specifica i requisiti che devono essere soddisfatti dall'organizzazione ai fini della rendicontazione in conformità agli Standard GRI. L'organizzazione inizia a utilizzare gli Standard GRI consultando [GRI 1](#).

[GRI 2: Informativa generale 2021](#) contiene informative che l'organizzazione utilizza per fornire dati in merito alle prassi di reportistica e ad altri dettagli organizzativi, quali attività, governance e normative.

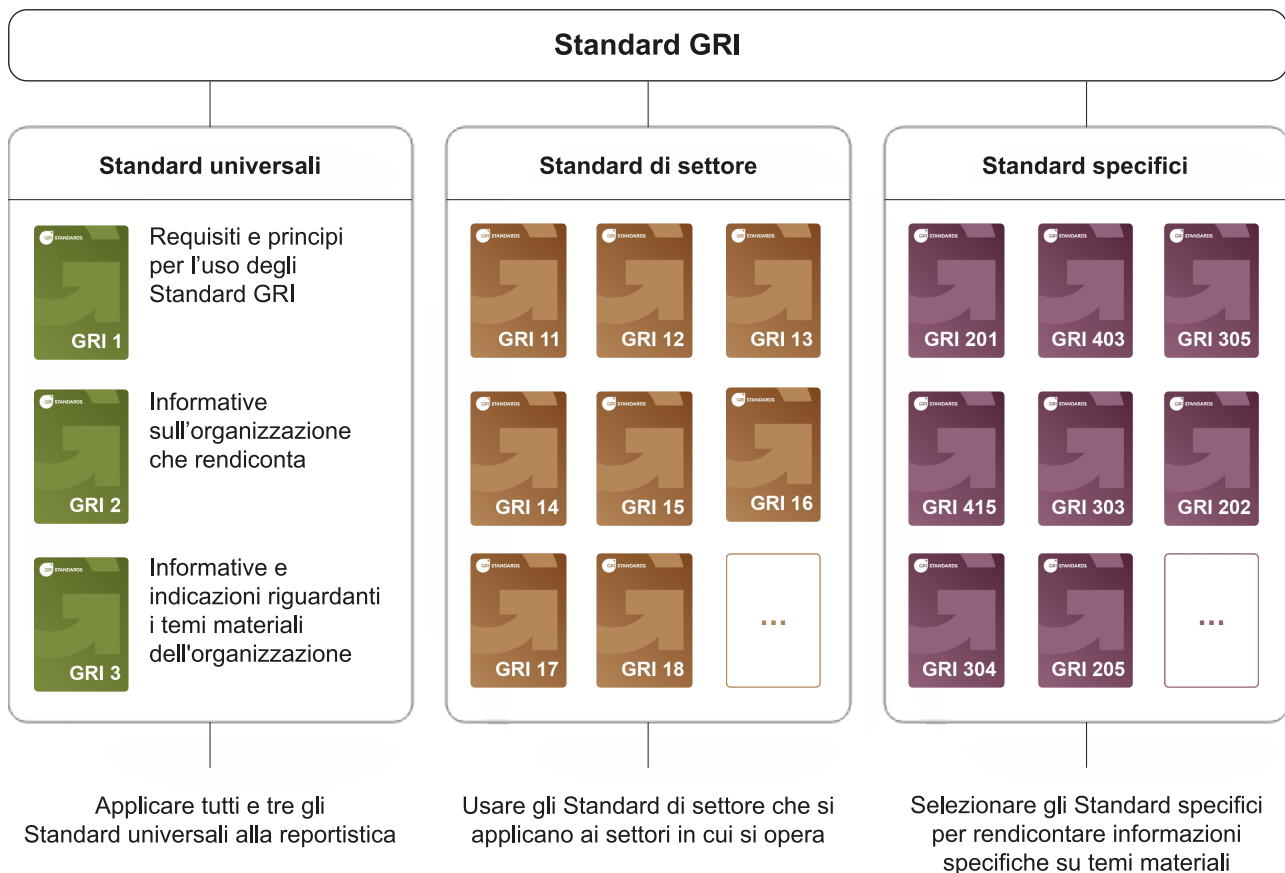
[GRI 3: Temi materiali 2021](#) offre indicazioni su come determinare i temi materiali. Contiene anche informative di cui l'organizzazione si serve per rendicontare dati relativi al processo volto a determinare i temi materiali, il loro elenco e il modo in cui gestisce ciascuno di essi.

### Standard di settore

Forniscono informazioni per le organizzazioni sui loro temi potenzialmente materiali. L'organizzazione usa gli Standard di settore che riguardano l'ambito in cui opera quando stabilisce i temi materiali e per decidere quali informazioni comunicare in merito.

### Standard specifici

Contengono informative per l'organizzazione in merito alla rendicontazione degli impatti relativi a temi specifici. L'organizzazione usa gli Standard specifici in base all'elenco di temi materiali che ha stabilito tramite lo standard [GRI 3](#).

**Figura 1. Standard GRI: Standard universali, di settore e specifici**

## Uso del presente Standard

Questo Standard può essere utilizzato da qualsiasi organizzazione – indipendentemente dalle dimensioni, dalla tipologia di attività svolta, dal settore, dall'ubicazione geografica o dall'esperienza di reportistica – per rendicontare informazioni sui suoi impatti correlati alla privacy dei clienti.

Un'organizzazione che prepara una rendicontazione in conformità agli Standard GRI deve rendicontare le seguenti informative, se ha determinato che la privacy dei clienti costituisce un tema materiale:

- [Informativa 3-3 in GRI 3: Temi materiali 2021](#) (vedere la clausola 1.1 in questo Standard);
- qualsiasi informativa presente in questo Standard specifico che sia attinente agli impatti sulla privacy dei clienti dell'organizzazione (Informativa 418-1).

Vedere [Requisiti 4 e 5 in GRI 1: Principi di rendicontazione 2021](#).

Per queste informative sono consentite ragioni di omissione.

Se l'organizzazione non può soddisfare un'informativa o un suo requisito (ad es., perché le informazioni richieste sono riservate o soggette a divieti normativi), deve specificare quale informativa o requisito non è in grado di rispettare e fornire una ragione dell'omissione insieme a una spiegazione nell'Indice dei contenuti GRI. Vedere il [Requisito 6 in GRI 1: Principi di rendicontazione 2021](#) per maggiori informazioni sulle ragioni alla base dell'omissione.

Se un'organizzazione non può rendicontare le informazioni necessarie in merito a una voce specificata in un'informativa perché tale voce (ad es., comitato, normativa, prassi, processo) non esiste, può soddisfare il requisito riportando questa ragione. L'organizzazione può spiegare i motivi per cui non possiede tale voce o descrivere eventuali piani per metterla in atto. L'informativa non impone all'organizzazione di attuare la voce in oggetto (ad es., sviluppare una normativa), ma solo di rendicontare che non esiste.

Se l'organizzazione intende pubblicare un report di sostenibilità a sé stante, non è necessario che ripeta informazioni già riportate pubblicamente altrove, come pagine web o nel report annuale. In questo caso, può rendicontare le informazioni necessarie fornendo un riferimento nell'indice dei contenuti GRI che indichi ove queste sono reperibili (ad es., tramite un link alla pagina web o menzionando la pagina della relazione annuale in cui sono state

pubblicate).

**Requisiti, linee guida e termini definiti**

Quanto segue si applica a questo Standard:

I requisiti sono indicati in **grassetto** e caratterizzati dal verbo "deve". Un'organizzazione deve attenersi ai requisiti per presentare una rendicontazione in conformità agli Standard GRI.

I requisiti possono essere accompagnati da linee guida.

Tali linee guida comprendono informazioni generali, spiegazioni ed esempi per aiutare l'organizzazione a comprendere meglio i requisiti stessi. L'organizzazione non ha l'obbligo di seguire tali linee guida.

Gli Standard possono anche contenere raccomandazioni. Si tratta di casi in cui si invita a seguire una particolare linea di condotta, ma senza alcun obbligo.

Il verbo "dovrebbe" indica una raccomandazione, mentre "può" indica una possibilità o una scelta.

I termini definiti sono sottolineati nel testo degli Standard GRI e collegati ipertestualmente alle rispettive definizioni nel [Glossario](#). L'organizzazione deve applicare le definizioni del Glossario.

# 1. Informativa sulla gestione del tema

Un'organizzazione che rendiconta in conformità agli Standard GRI deve specificare come gestisce ciascuno dei suoi temi materiali.

Se un'organizzazione ha determinato che la privacy dei clienti costituisce un tema materiale, deve rendicontare come lo gestisce utilizzando l'[Informativa 3-3 in GRI 3: Temi materiali 2021](#) (vedere la clausola 1.1 in questa sezione).

Questa sezione è quindi concepita per integrare - non sostituire - l'Informativa 3-3 in *GRI 3*.

---

**REQUISITI**      **1.1**      **L'organizzazione deve rendicontare come gestisce la privacy dei clienti utilizzando l'[Informativa 3-3 in GRI 3: Temi materiali 2021](#).**

## 2. Informativa sul tema

### Informativa 418-1 Denunce comprovate riguardanti le violazioni della privacy dei clienti e perdita di dati dei clienti

---

**REQUISITI**

L'organizzazione deve rendicontare le seguenti informazioni:

- a. Numero totale di denunce comprovate ricevute riguardo a violazioni della privacy dei clienti, suddivisi per:
  - i. reclami ricevuti da terze parti e comprovati dall'organizzazione;
  - ii. reclami da organi normativi.
- b. Numero totale di episodi identificati di fuga, furto o perdita di dati dei clienti.
- c. Se l'organizzazione non ha individuato alcun reclamo fondato, sarà sufficiente una breve dichiarazione in merito.

#### Requisiti di compilazione

- 2.1 Nel compilare le informazioni indicate nell'Informativa 418-1, l'organizzazione deve rendicontare se un numero significativo di tali violazioni si riferisce a eventi risalenti agli anni precedenti.

---

**LINEE GUIDA**

#### Background

La protezione della privacy di clienti è un obiettivo generale riconosciuto in regolamenti nazionali e normative delle organizzazioni. Come definito nel documento dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) *'Linee guida per le imprese multinazionali*, ci si aspetta che le organizzazioni 'rispettino la privacy dei clienti e adottino misure ragionevoli per assicurare la sicurezza dei dati personali che raccolgono, conservano, elaborano o divulgano'.

Per proteggere la privacy dei clienti, ci si aspetta che un'organizzazione limiti la raccolta di dati personali, esegua tale raccolta con mezzi legittimi e sia trasparente riguardo alla raccolta, uso e protezione dei dati. Ci si aspetta inoltre che l'organizzazione non divulghi o usi informazioni personali dei clienti per scopi diversi da quelli concordati, e che informi direttamente i clienti di eventuali modifiche nelle normative o misure di protezione dei dati.

La presente informativa offre una valutazione del successo di sistemi e procedure di gestione relativamente alla tutela della privacy dei clienti.



# Glossario

Questo glossario fornisce definizioni di termini utilizzati nel presente Standard. L'organizzazione deve applicare queste definizioni quando usa gli Standard GRI.

Le definizioni incluse in questo glossario possono contenere termini che sono ulteriormente definiti nel [Glossario degli Standard GRI](#) completo. Tutti i termini definiti sono sottolineati. Se un termine non è definito in questo Glossario e neppure nel [Glossario degli Standard GRI](#) completo, si applicano definizioni comunemente utilizzate e comprese.

---

## D

### denunce comprovate

Comunicazione scritta da parte di un'Autorità o un analogo Organo Pubblico di Vigilanza, rivolta all'organizzazione che identifica le [violazioni della privacy dei clienti](#) o una denuncia presentata all'organizzazione che sia stato riconosciuto come legittima da questa.

### diritti umani

Diritti intrinseci di tutte le persone che includono perlomeno quelli definiti nella *Carta internazionale dei diritti umani delle Nazioni Unite (ONU)* e i principi concernenti i diritti fondamentali definiti nella *Dichiarazione sui diritti e principi fondamentali sul lavoro dell'Organizzazione internazionale del lavoro (ILO)*.

Fonte: Nazioni Unite (ONU), *Principi guida su imprese e diritti umani: attuare il Quadro di riferimento delle Nazioni Unite "Proteggere, Rispettare e Rimediare"*, 2011; modificato

Nota: Si vedano le [Indicazioni per il punto 2-23-b-i in GRI 2: Informativa generale 2021](#) per maggiori informazioni su 'diritti umani'.

---

## I

### impatto

Effetto che l'organizzazione ha o potrebbe avere sull'economia, sull'ambiente e sulle persone, compreso sui loro [diritti umani](#), che a sua volta può indicarne il contributo (negativo o positivo) allo [sviluppo sostenibile](#).

Nota 1: Gli impatti possono essere effettivi o potenziali, negativi o positivi, a breve o a lungo termine, intenzionali o non intenzionali, reversibili o irreversibili.

Nota 2: Si veda la sezione [2.1 in GRI 1: Principi di rendicontazione 2021](#) per maggiori informazioni su 'impatto'.

---

## P

### privacy dei cliente

Diritto del cliente alla privacy e alla propria dimensione personale.

Esempi: L'obbligo di osservare la confidenzialità, la protezione di dati, la protezione di informazioni o dati da abuso o furto, l'uso di informazioni o dati per il solo scopo previsto originale se non concordato specificamente in altro modo.

Nota: È inteso che i clienti sono sia clienti finali (consumatori) che clienti business-to-business.

---

## S

### sviluppo sostenibile / sostenibilità

Lo sviluppo che è in grado di soddisfare i bisogni della generazione presente, senza compromettere la possibilità che le generazioni future riescano a soddisfare i propri.

Fonte: Commissione mondiale sull'ambiente e lo sviluppo, *Our Common Future*, 1987

Nota: I termini 'sostenibilità' e 'sviluppo sostenibile' sono utilizzati in modo intercambiabile negli Standard GRI.

---

## T

### temi materiali

Temì che rappresentano gli [impatti](#) dell'organizzazione sull'economia, sull'ambiente e sulle persone, inclusi quelli sui loro [diritti umani](#).

Nota: Si veda la [sezione 2.2 in GRI 1: Principi di rendicontazione 2021](#) e la [sezione 1 in GRI 3: Temi materiali 2021](#) per maggiori informazioni su 'temi materiali'.

---

**V****violazione della privacy dei clienti**

Mancata conformità alle disposizioni legali esistenti e alle norme (volontarie) sulla protezione della [privacy dei clienti](#).

## Bibliografia

La presente sezione elenca gli strumenti intergovernativi autorevoli utilizzati per lo sviluppo del presente Standard.

### Strumenti autorevoli

1. Organizzazione per la cooperazione e lo sviluppo economico (OCSE), *Linee guida per le imprese multinazionali*, 2011.



Casella postale 10039  
1001 EA Amsterdam  
Paesi Bassi

[www.globalreporting.org](http://www.globalreporting.org)