

# GRI 418 : 客户隐私 2016

# 418

生效日期：7/1/2018

议题标准

# GRI 418 : 客户隐私 2016

## 议题标准

### 生效日期

本标准对以下日期或之后出版的报告或其他材料有效 7/1/2018.

### 责任

本标准由全球可持续发展标准委员会 ( GSSB ) 发布。关于GRI标准的任何反馈可发送至 [gssbsecretariat@globalreporting.org](mailto:gssbsecretariat@globalreporting.org)，以供GSSB考量。

### 正当程序

本文件是出于公共利益并根据GSSB正当程序协议的要求而制定。本文件采用了多利益相关方的专业知识，并考虑到权威政府间文件以及对组织在社会、环境和经济责任方面的广泛期望。

### 法律责任

本文件旨在促进可持续发展报告的编制，由全球可持续发展标准委员会 ( GSSB ) 通过独特的多利益相关方磋商过程来制定，涉及世界各地众多组织的代表和报告信息使用者。虽然 GRI 董事会和 GSSB 鼓励所有组织使用 GRI 可持续发展报告标准 ( 简称 GRI 标准 ) 和相关解释，但完全或部分基于 GRI 标准及相关解释来编制和发布的报告，仍由报告编制组织自身全权负责。对于在编制报告的过程中因使用 GRI 标准和相关解释而直接或间接导致的任何后果或损害，以及在使用基于 GRI 标准和相关解释的报告中直接或间接导致的任何后果或损害，GRI 董事会、GSSB 和 Stichting Global Reporting Initiative ( GRI ) 概不负责。

### 版权和商标声明

本文件受 Stichting Global Reporting Initiative ( GRI ) 的版权保护。允许在未经 GRI 事先许可的情况下，复制和分发本文件以供参考和 / 或用于编制可持续发展报告。但是，未经 GRI 事先书面许可，不得以任何形式或通过任何方式 ( 电子、机械、影印、录制或其他方式 ) 复制、存储、翻译或转让本文件及其摘录。

Global Reporting Initiative、GRI 及其徽标、GSSB 及其徽标以及 GRI Sustainability Reporting Standards ( GRI Standards ) 是 Stichting Global Reporting Initiative 的商标。

# 简介

*GRI 418：客户隐私 2016* 包含一系列披露项，用于组织报告其客户隐私相关影响，以及管理影响的方法。

本标准的结构如下：

- **第1节** 包含一个要求，说明组织如何管理其客户隐私相关的影响。
- **第2节** 包含一个披露项，说明组织的客户隐私相关影响。
- **术语表** 包括在GRI标准中具有特定含义的术语。这些术语在GRI标准的正文中以下划线标出，并链接至相应的定义。
- **参考文件** 列出了制定本标准时使用的权威政府间文件。

简介的其余部分提供议题背景，概述GRI标准体系，并提供关于使用本标准的更多信息。

## 议题背景

本标准是关于 客户隐私 议题，包括丢失客户资料和侵犯客户隐私。导致这些情况的原因，可能是未遵守关于客户隐私保护的现行法律法规和/或其他自愿性标准。

经济合作与发展组织的重要文件中介绍了这些概念：参见[参考文件](#)。

## GRI标准体系

本标准是GRI可持续发展报告标准（GRI标准）的一部分。GRI标准使组织能够报告对经济、环境和人最重大的影响，包括对人权的影响，以及管理影响的方法。

GRI标准是由相互关联的多套标准组成的系统，分为三个系列：GRI通用标准、GRI行业标准和GRI议题标准（见本标准的图1）。

### 通用标准：GRI 1、GRI 2和GRI 3

*GRI 1：基础2021* 规定了组织符合GRI标准编制报告必须遵守的要求。组织首先查阅*GRI 1*，开始使用GRI标准。

*GRI 2：一般披露2021* 包含一系列披露项，用于组织说明报告实践和其他组织详情（例如活动、管治和政策）。

*GRI 3：实质性议题2021* 就确定实质性议题提供指导。还包含一系列披露项，用于组织说明其确定实质性议题的过程、实质性议题清单以及每个议题的管理方法。

### 行业标准

行业标准为组织提供信息，以确定可能的实质性议题。组织在确定实质性议题以及为实质性议题报告哪些信息时，采用适用于所在行业的行业标准。

### 议题标准

议题标准包含一系列披露项，用于组织报告与具体议题有关影响的信息。组织使用*GRI 3*确定实质性议题清单，并据此采用议题标准。

图1.GRI标准：通用、行业和议题标准





## 使用本标准

任何组织——不论规模、类型、行业、地理位置或报告经验——皆可使用本标准报告其客户隐私 相关的影响。

如果组织要编制符合GRI标准的报告，确定客户隐私为实质性议题，需要报告以下披露项：

- [GRI 3：实质性议题 2021](#) 的披露项 3-3（见本标准条款1.1）；
- 本议题标准中涉及组织的客户隐私相关影响的任何披露项（披露项418-1）。

见[GRI 1：基础2021](#)的要求4 和 5。

此等披露项允许有从略的原因。

如果无法遵守披露项或披露项中的要求（例如，由于必要信息保密或被法律禁止），组织就需要说明其无法遵守的披露项或要求，并在GRI内容索引中提供从略的原因及解释。关于从略原因的更多信息，参见[GRI 1：基础2021](#)中的要求6。

如果由于某个条目（例如，委员会、政策、做法、流程）不存在，无法报告披露项中条目的必要信息，组织可说明这一情况以遵守要求。组织可解释没有相关条目的原因，或说明任何建立相关条目的计划。披露项并不要求组织实施条目（例如，制定政策），但如果条目不存在，则要求组织报告。

如果组织计划发布单独的可持续发展报告，那么无需重复已在别处公开报告的信息，例如网页或年度报告。在这种情况下，组织可在GRI内容索引中提供参考，说明何处可找到该等信息（例如，提供网页链接或引用年度报告中已发布信息的页面），从而报告规定的披露项。

### 要求、指南和定义的术语

以下内容适用于本标准：

要求以**粗体字**标明，并用“应”表示。组织必须遵守要求，以符合GRI标准编制报告。

要求可能附有指南。

指南包括背景信息、解释和示例，有助于组织更好地理解要求。但不要求组织遵守指南。

标准还可能包括建议，即鼓励采取但并非要求的具体行动。

“宜”表示建议，“可”表示可能或可选。

定义的术语在 GRI标准的正文中以下划线标出，并链接至[术语表中相应的定义](#)。组织需要采用术语表中的定义。

## 1.议题管理披露项

如果组织要编制符合GRI标准的报告，需要报告其管理每项实质性议题的方法。

确定客户隐私为实质性议题的组织，需要使用[GRI 3：实质性议题 2021](#) 的披露项 3-3，报告其管理议题的方法（见本节条款1.1）。

因此，本节旨在补充——而非取代——[GRI 3](#)的披露项3-3。

**要求** 1.1 组织应使用GRI 3：实质性议题2021的披露项3-3，报告对客户隐私的管理方法。

## 2.议题披露项

## 披露项 418-1 涉及侵犯客户隐私和丢失客户资料的经证实的投诉

### 要求

组织应报告以下信息：

- a. 收到的 经证实的投诉（涉及 侵犯客户隐私），分类如下：
  - i. 来自外部且经组织证实的投诉；
  - ii. 来自监管机构的投诉。
- b. 经确认的泄露、失窃或丢失客户资料的总数。
- c. 如果组织未发现任何经证实的投诉，简要说明这一事实即可。

编制要求：

- 2.1 编制披露项 418-1 规定的信息时，如果大量此等违规与之前年度的事件有关，组织应予以指出。

### 指南

#### 背景

保护客户隐私是在国家法规和组织政策中普遍认可的目标。经济合作与发展组织（OECD）的《*OECD 跨国企业准则*》中规定，组织应当“尊重消费者隐私，并采取合理措施确保收集、存储、处理或传播个人资料的安全”。

为保护客户隐私，组织应当限制对个人数据的收集，以合法途径收集数据，并对收集、使用和保护数据的方式保持透明。除非经客户同意，组织不应透露客户个人信息，不将客户个人信息用于除约定之外的任何目的，并将资料保护政策或措施的任何变化直接传达给客户。

本披露项可评估与客户隐私保护相关的管理体系和程序成功与否。

## 术语表

本术语表为GRI标准中使用的术语提供定义。组织在使用GRI标准时，需采用这些定义。

本术语表可能包含在完整 [GRI 标准术语表](#) 中详细定义的术语。所有已定义的术语均以下划线表示。如果某个术语在本术语表或完整 [GRI 标准术语表](#) 中未给出定义，则可采用通常所理解的常用定义。

#### 人权

所有人固有的权利，至少包括联合国《*国际人权宪章*》中规定的权利和国际劳工组织《*关于工作中基本原则和权利宣言*》中规定的基本权利原则

来源：联合国（UN），《*工商企业与人权指导原则：实施联合国“保护、尊重和补救”框架*》，2011年；经修订

注：关于“人权”的更多信息，参见 [GRI 2：一般披露 2021](#) 中对2-23-b-i的指南

#### 侵犯客户隐私

未遵守保护客户隐私的现行法律规定和（自愿）标准

#### 可持续发展 / 可持续性

满足当代人需求又不损害子孙后代的需求

来源：世界环境与发展委员会，《*我们共同的未来*》，1987年

注：在 GRI 标准中，“可持续性”和“可持续发展”可以互换使用。

#### 实质性议题

体现组织对经济、环境和人的最重大影响（包括对人权影响）的议题

注：关于“实质性议题”的更多信息，请参见 [GRI 1：基础 2021](#) 中的2.2 节，以及 [GRI 3：实质性议题 2021](#) 中的第1节

#### 客户隐私

#### 客户关于隐私和个人庇护的权利

示例： 保密义务；数据保护；保护信息或数据免遭误用或被窃；除非另有明确约定，否则仅允许将信息或数据用于最初预期目的

注： 客户应包括最终客户（消费者）以及B2B客户。

#### 影响

组织对经济、环境和 / 或人已经或可能产生的影响，包括对人权的影响，可表明其对可持续发展的作用（正面或负面）

注1： “影响”一词可指实际或潜在、正面或负面、短期或长期、有意或无意、可逆或不可逆的影响。

注2： 关于“影响”的更多信息，参见[GRI 1: 基础 2021](#)的2.1 节

#### 经证实的投诉

监管机构或类似官方机构向组织发出的确定侵犯 客户隐私的书面声明，或向组织提出的已被组织认定为合理的投诉

本节列出制定本标准时使用的权威性政府间文件。

#### 权威性文件：

1. 经济合作与发展组织（OECD），《*OECD 跨国企业准则*》，2011年。



GRI  
PO Box 10039,  
1001 EA Amsterdam,  
The Netherlands

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