



GRI STANDARDS

GRI 418: 고객 개인정보보호 2016

418

EFFECTIVE DATE: 1 JULY 2018

TOPIC STANDARD

GRI 418: 고객 개인정보 보호 2016

주제 표준

발효일

이 표준은 2018년 7월 1일 이후에 발행되는 보고서 또는 기타 자료에 적용됩니다.

책임

이 표준은 글로벌 지속가능성 표준 위원회(GSSB)에서 발행합니다. GRI 표준에 대한 피드백은 gssbsecretariat@globalreporting.org 으로 제출하여 GSSB의 검토를 받을 수 있습니다.

적용 절차

이 표준은 공공의 이익을 위해 GSSB 적용 절차 프로토콜의 요구사항에 따라 개발되었습니다. 이 표준은 여러 이해관계자의 전문성과 권위 있는 정부 간 기구 및 사회적, 환경적, 경제적 책임과 관련된 조직의 광범위한 기대치를 고려하여 개발되었습니다.

법적 책임

지속가능성 보고를 촉진하기 위해 고안된 이 문서는 글로벌 지속가능성 표준위원회(GSSB)가 전 세계 조직 대표와 보고서 정보 사용자가 참여하는 고유한 다중 이해관계자 협의 과정을 통해 개발했습니다. GRI 이사회와 GSSB는 모든 조직이 GRI 지속가능성 보고 표준(GRI Standards) 및 관련 해석을 사용할 것을 권장하지만, GRI 표준 및 관련 해석을 전부 또는 부분적으로 기반으로 보고서를 작성 및 발행하는 것은 전적으로 보고서 작성자의 책임입니다. GRI 이사회, GSSB 또는 GRI(글로벌 보고 이니셔티브)는 보고서 작성 시 GRI 표준 및 관련 해석을 사용하거나 GRI 표준 및 관련 해석에 기반한 보고서 사용으로 인해 직간접적으로 발생하는 결과 또는 손해에 대해 책임을 지지 않습니다.

저작권 및 상표 고지

이 문서는 GRI(Global Reporting Initiative)에 의해 저작권이 보호됩니다. GRI의 사전 허가 없이 정보 제공 및/또는 지속가능성 보고서 작성에 사용하기 위해 이 문서를 복제 및 배포하는 것은 허용됩니다. 그러나 본 문서 또는 본 문서에서 발췌한 내용은 GRI의 사전 서면 허가 없이 다른 목적으로 어떠한 형태나 수단(전자, 기계, 복사, 녹음 또는 기타)으로도 복제, 저장, 번역 또는 전송할 수 없습니다.

글로벌 리포팅 이니셔티브, GRI 및 로고, GSSB 및 로고, GRI 지속가능성 보고 표준(GRI Standards) 및 로고는 스티칭 글로벌 리포팅 이니셔티브의 상표입니다.

목차

소개	4
1. 주제 관리 공시	7
2. 주제 공개	8
공개 418-1 고객 개인정보 침해와 관련된 입증된 불만 사항 개인정보 및 고객 데이터 손실	8
용어집	9
참고 문헌	11

소개

*GRI 418: 고객 개인정보 보호 2016*에는 조직이 고객 개인정보 보호와 관련된 영향을 이러한 영향을 관리하는 방법에 대한 정보를 보고할 수 있는 공개 사항이 포함되어 있습니다.

이 표준은 다음과 같이 구성되어 있습니다:

- **섹션 1**에는 조직이 고객 개인정보 보호 관련 영향을 관리하는 방법에 대한 정보를 제공하는 요구사항이 포함되어 있습니다.
- **섹션 2**에는 조직의 고객 개인정보 관련 영향에 대한 정보를 제공하는 하나의 공개가 포함되어 있습니다.
- **용어집**에는 GRI 표준에서 사용되는 특정 의미를 가진 정의된 용어가 포함되어 있습니다. 용어는 GRI 표준 본문에서 밑줄이 그어져 있으며 정의에 링크되어 있습니다.
- **참고 문헌**에는 이 표준을 개발하는 데 사용된 권위 있는 정부 간 기구가 나열되어 있습니다.

나머지 소개 섹션에서는 주제에 대한 배경, GRI 표준 시스템에 대한 개요 및 본 표준 사용에 대한 추가 정보를 제공합니다.

주제에 대한 배경

본 표준은 관한 주제를 다룹니다. 고객 데이터 손실 및 등 고객 프라이버시에 고객 프라이버시 침해. 이는 고객 개인정보 보호에 관한 기존 법률, 규정 및/또는 기타 자발적 표준을 준수하지 않아서 발생할 수 있습니다.

이러한 개념은 경제협력개발기구의 주요 문서에서 다루고 있습니다([참고 문헌](#) 참조).

GRI 표준 체계

이 표준은 GRI 지속가능성 보고 표준(GRI Standards)의 일부입니다. GRI 표준을 통해 조직은 인권에 대한 영향을 포함하여 경제, 환경, 사람에 미치는 가장 중요한 영향과 이러한 영향을 관리하는 방법에 대한 정보를 보고할 수 있습니다.

GRI 표준은 세 가지 시리즈로 구성된 상호 연관된 표준의 시스템으로 구성되어 있습니다: GRI 보편 표준, GRI 섹터 표준, GRI 주제 표준(본 표준의 [그림 1](#) 참조).

범용 표준: GRI 1, GRI 2 및 GRI 3

*GRI 1: 재단 2021*은 조직이 GRI 표준에 따라 보고하기 위해 준수해야 하는 요구사항을 명시합니다. 조직은 *GRI 1*을 참조하여 GRI 표준을 사용하기 시작합니다.

*GRI 2: 일반 공개 2021*에는 조직이 활동, 거버넌스 및 정책과 같은 보고 관행 및 기타 조직 세부 정보에 대한 정보를 제공하기 위해 사용하는 공개 내용이 포함되어 있습니다.

*GRI 3: 중요 주제 2021*은 중요 주제를 결정하는 방법에 대한 지침을 제공합니다. 또한 조직이 중요 주제 결정 프로세스, 중요 주제 목록 및 각 주제를 관리하는 방법에 대한 정보를 보고하는 데 사용하는 공시가 포함되어 있습니다.

부문 표준

부문별 표준은 조직이 중요하게 다룰 수 있는 주제에 대한 정보를 제공합니다. 조직은 중요 주제를 결정할 때와 각 중요 주제에 대해 보고할 내용을 결정할 때 해당 부문에 적용되는 부문 표준을 사용합니다.

주제 표준

주제 표준에는 조직이 특정 주제와 관련된 영향에 대한 정보를 보고하는 데 사용하는 공개 사항이 포함되어 있습니다. 조직은 *GRI 3*을 사용하여 결정한 중요 주제 목록에 따라 주제 표준을 사용합니다.

그림 1. GRI 표준: 범용, 부문 및 주제 표준



이 표준 사용하기

이 표준은 규모, 유형, 업종, 지리적 위치 또는 보고 경험에 관계없이 모든 조직이 고객 개인정보와 관련된 영향에 대한 정보를 보고하는 데 사용할 수 있습니다.

GRI 표준에 따라 보고하는 조직은 고객 개인정보 보호를 중요한 주제로 판단한 경우 다음 공개 사항을 보고해야 합니다:

- **GRI 3: 중요 주제 2021의 공개 3-3**(본 표준의 1.1항 참조);
- 조직의 고객 개인정보 보호 관련 영향과 관련된 이 주제 표준의 모든 공개(공개 418-1).

GRI 1: 기초 2021의 요구사항 4 및 5를 참조하세요. 이러한 공개에는 생략 사유가 허용됩니다.

조직이 공개 또는 공개 요구사항을 준수할 수 없는 경우(예: 필요한 정보가 기밀이거나 법적 금지의 대상이 되는 경우), 조직은 준수할 수 없는 공개 또는 요구사항을 명시하고 GRI 내용 색인에 설명과 함께 생략 사유를 제공해야 합니다. 생략 사유에 대한 자세한 내용은 **GRI 1: 기초 2021의 요구사항 6**을 참조하세요.

조직이 공개에 명시된 항목(예: 위원회, 정책, 관행, 프로세스)이 존재하지 않아 해당 항목에 대한 필수 정보를 보고할 수 없는 경우, 이를 실제로 보고하여 요건을 준수할 수 있습니다. 조직은 해당 항목이 없는 이유를 설명하거나 해당 항목을 개발할 계획을 설명할 수 있습니다. 공개는 조직이 해당 항목을 구현(예: 정책 개발)할 것을 요구하지 않으며, 해당 항목이 존재하지 않는다고 보고하는 것만으로 충분합니다.

조직이 독립형 지속가능성 보고서를 발행하려는 경우, 웹 페이지나 연례 보고서 등 다른 곳에서 이미 공개적으로 보고한 정보를 반복할 필요가 없습니다. 이러한 경우, 조직은 GRI 콘텐츠 색인에 해당 정보를 찾을 수 있는 위치에 대한 참조를 제공하여(예: 웹 페이지 링크를 제공하거나 해당 정보가 게시된 연례 보고서의 페이지를 인용) 필수 공개를 보고할 수 있습니다.

요구사항, 지침 및 정의된 용어

이 표준 전체에 적용되는 내용은 다음과 같습니다:

요건은 **굵은 글씨체로** 표시되며 '하여야 한다'라는 단어로 표시됩니다. 조직은 GRI 표준에 따라 보고하기 위해 요구사항을 준수해야 합니다.

요구사항에는 지침이 수반될 수 있습니다.

지침에는 조직이 요구사항을 더 잘 이해할 수 있도록 배경 정보, 설명 및 예시가 포함됩니다. 조직이 지침을 반드시 준수할 필요는 없습니다.

표준에는 권장 사항도 포함될 수 있습니다. 이는 특정 행동 방침을 권장하지만 필수는 아닌 경우입니다.

'should'라는 단어는 권장 사항을 나타내고, 'can'이라는 단어는 가능성 또는 옵션을 나타냅니다.

정의된 용어는 GRI 표준 본문에서 말줄이 그어져 있으며 [용어집의](#) 정의에 링크되어 있습니다. 조직은 용어집의 정의를 적용해야 합니다.

1. 주제 관리 공개

GRI 표준에 따라 보고하는 조직은 각 중요 주제를 어떻게 관리하는지 보고해야 합니다.

고객 개인정보 보호를 중요 주제로 결정한 조직은 *GRI 3: 2021의 공개 3-3: 중요 주제*(이 섹션의 1.1항 참조)를 사용하여 해당 주제를 어떻게 관리하는지 보고해야 합니다.

따라서 이 섹션은 *GRI 3의 공개 3-3*을 대체하는 것이 아니라 보완하기 위해 작성되었습니다.

요구사항	1.1	보고 조직은 <i>GRI 3: 중요 주제 2021의 공개 3-3</i> 을 사용하여 <u>고객 개인정보</u> 관리 방법을 보고해야 합니다.
------	-----	--

2. 주제 공개

공개 418-1 고객 프라이버시 침해 및 고객 데이터 손실에 관한 입증된 불만 사항

요구사항

보고 조직은 다음 정보를 보고해야 합니다:

- a. 고객 개인정보 침해와 관련하여 접수된 입증된 불만 기준으로 분류한 수치입니다: 총 건수를
 - i. 외부 당사자로부터 접수되어 조직이 입증한 불만 건수
 - ii. 규제 기관의 불만 사항
- b. 고객 데이터의 유출, 도난 또는 손실이 확인된 총 건수.
- c. 조직에서 입증된 불만 사항을 확인하지 못한 경우에는 이 사실에 대한 간략한 설명으로 충분합니다.

컴파일 요구 사항

- 2.1 공시 418-1에 명시된 정보를 작성할 때 보고 조직은 이러한 침해 중 상당수가 이전 연도의 사건과 관련이 있는지 표시해야 합니다.

지침

배경

고객 개인정보 보호는 국가 규정 및 조직 정책에서 일반적으로 인정되는 목표입니다. 경제협력개발기구(OECD)의 *다국적 기업을 위한 OECD 가이드라인*에 명시된 대로 조직은 '소비자 개인정보를 존중하고 수집, 저장, 처리 또는 유포하는 개인정보의 보안을 보장하기 위해 합리적인 조치를 취해야 한다'고 규정하고 있습니다.

고객의 개인정보를 보호하기 위해 조직은 개인 데이터 수집을 제한하고 합법적인 방법으로 데이터를 수집하며 데이터 수집, 사용 및 보호 방법에 대해 투명하게 공개해야 합니다. 또한 동의한 목적 이외의 용도로 개인 고객 정보를 공개하거나 사용하지 않아야 하며, 데이터 보호 정책이나 조치의 변경 사항을 고객에게 직접 알려야 합니다.

이 공개는 고객 개인정보 보호와 관련된 관리 시스템 및 절차의 성공 여부에 대한 평가를 제공합니다.

용어집

이 용어집은 본 표준에서 사용되는 용어에 대한 정의를 제공합니다. 조직은 GRI 표준을 사용할 때 이러한 정의를 적용해야 합니다.

이 용어집에 포함된 정의에는 *GRI 표준 용어집* 전체에 추가로 정의된 용어가 포함될 수 있습니다. 정의된 모든 용어에는 밑줄이 그어져 있습니다. 본 용어집 또는 *GRI 표준* 전체에 정의되지 않은 용어의 경우 *용어집* 일반적으로 사용되고 이해되는 정의가 적용됩니다.

B	고객 개인정보 침해	<u>고객 개인정보 보호</u> 에 관한 기존 법적 규정 및 (자발적) 표준 미준수
	고객 개인정보	프라이버시 및 개인적 피난처에 대한 고객의 권리
C		예: 기밀 준수 의무, 데이터 보호, 오용 또는 도난으로부터 정보 또는 데이터 보호, 특별히 달리 합의하지 않는 한 정보 또는 데이터를 원래 의도된 목적으로만 사용해야 함
	참고:	고객에는 B2B 고객뿐만 아니라 최종 고객(소비자)도 포함되는 것으로 이해됩니다.
H	인권	모든 인간에게 내재된 권리로, 최소한 <i>국제연합(UN)</i> 국제인권장전에 명시된 권리를 포함한다. <i>국제연합(UN)</i> <i>국제인권장전</i> 에 명시된 권리 및 <i>국제노동기구(LO)</i> <i>기본 원칙 및 권리 선언</i> 에 명시된 기본권 관련 원칙을 포함합니다.
	출처:	유엔(UN), <i>기업과 인권에 관한 기본 원칙: 유엔 "보호, 존중 및 구제" 프레임워크 이행</i> , 2011; 수정됨
	참고:	'인권'에 대한 자세한 내용은 <i>GRI 2: 일반 공개 2021의 2-23-b-i 지침</i> 을 참조하세요.
I	영향	조직이 경제, 환경, 사람에 미치는 또는 미칠 수 있는 영향, 다음을 포함합니다. 그들의 <u>인권</u> , 그리고 <u>지속 가능한 발전</u> 에 대한 기여도(부정적 또는 긍정적)를 나타낼 수 있습니다.
	참고 1:	영향은 실제 또는 잠재적, 부정적 또는 긍정적, 단기 또는 장기, 의도적 또는 비의도적, 가역적 또는 비가역적일 수 있습니다.
	참고 2:	'영향'에 대한 자세한 내용은 <i>GRI 1: 기초 2021의 2.1</i> 을 섹션 참조하세요.
M	중요 주제	경제, 환경, 사람에 대한 조직의 가장 중요한 영향을 나타내는 주제입니다, <u>인권</u> 에 대한 영향을 포함하여 사람들에게 미치는 중대한 영향을 나타내는 주제
	참고:	'중요 주제'에 대한 자세한 내용은 <i>GRI 1: 기초 2021의 섹션 2.2</i> 및 <i>GRI 3: 중요 주제 섹션 1</i> 을 2021의 참조하십시오.
S	입증된 불만	규제 기관 또는 이와 유사한 공식 기관이 조직에 보낸 서면 진술서로서 다음과 같은 내용이 포함되어야 합니다. <u>고객 개인정보 침해</u> 또는 조직에 제기된 불만이 조직에 의해 합법적인 것으로 인정된 것을 식별합니다.
	지속 가능한 개발/지속 가능성	미래 세대가 자신의 필요를 충족할 수 있는 능력을 손상시키지 않으면서 현재의 필요를 충족하는 개발
	출처:	세계 환경 및 개발 위원회, <i>우리 공동의 미래</i> , 1987년

참고: GRI 표준에서는 '지속가능성'과 '지속가능한 개발'이라는 용어를 같은 의미로 사용합니다.

참고 문헌

이 섹션에는 이 표준을 개발하는 데 사용된 권위 있는 정부 간 기구가 나열되어 있습니다.

권위 있는 기구:

1. 경제협력개발기구(OECD), *다국적 기업을 위한 OECD 가이드라인*, 2011.



PO Box 10039

1001 EA 암스테르담 네덜란드

www.globalreporting.org