

HRMI 数据保护和隐私政策

HRMI 需要收集您的个人信息及敏感信息，这是完善我们的公民权利和政治权利指标的部分要求。以下的两组数据是分开存储的：

1. 个人信息，包括潜在专家调查问卷受访者及其提名者的姓名和联系方式。
2. 年度专家调查问卷的调查结果（不识别身份/匿名）。

您有权向我们索取我们保存的与您有关的任何个人信息的副本，如果您认为这些信息有误，则有权要求对其进行更正或永久删除。如果您想索取相关信息的副本，或者想更正或永久删除相关信息，请通过 survey@humanrightsmeasurement.org 联系我们 以下内容将说明我们如何保护上述信息的安全。

1. 潜在调查受访者的姓名和联系方式

此信息分两个阶段采集。首先，可以由 HRMI 任命的大使（这些大使是我们的本地合作伙伴，值得信赖的合作伙伴组织的人员，有时甚至是现有调查的受访者）提名（通过安全的在线表格）人权从业人员参加调查。被提名人员会被询问是否希望参加调查。如果同意，他们可以通过安全的在线同意书提供其姓名和电子邮件地址。我们的安全政策的主要特点是：

- 所有在线表单都托管在 HRMI 网站上，该网站具有 SSL 证书并受 https 安全保护。这意味着信息在传输中是安全的（加密的）。
- 通过同意书提交的姓名和电子邮件将直接（加密）发送到我们的客户关系管理（CRM）软件。基于云科技的客户管理软件已通过所有相关安全 ISO 标准的认证，包括 27001、27017 和 27018，以确保所有信息能以加密方式捕获、管理和保留。客户管理软件系统的访问权限仅限于由位于新西兰的 HRMI 工作人员组成的一个小组。
- HRMI 使用这些信息向这些潜在的调查对象中的每个人发送一个 HRMI 在线专家调查问卷的唯一链接。
- 被提名参加调查但未填写同意书的人员的名称不会添加到 CRM 数据库中，而且，所有提名的详细信息都将在每年调查征募期结束时被删除。

2. 调查问卷的答复

该调查托管在 [Qualtrics](https://www.qualtrics.com) 网站上，该网站具有 SSL 证书，并受 https 安全保护。这意味着所有输入和传输的信息都是加密的。IP 地址不会被储存。只有位于佐治亚大学（UGA）全球问题研究中心（GLOBIS）中一个由 HRMI 工作人员组成的小组能够访问 Qualtrics 调查答复数据。

对受访者进行调查的主要潜在风险是，如果他们的电子邮件被黑客入侵或受到监视，敌对分子可能会看到他们正在与 HRMI 进行交流，并且知道他们可能对我们的公民政治权利指标所作的工作。¹但是他们不太可能能够访问提交的调查信息本身。唯一的例外是，如果被调查者处于监控之下，其中包括例如键盘记录监控等，那么在这种情况下，

某些被调查者在调查中的输入可能是不安全的。如果受访者对此有所担心，我们强烈建议受访者使用可以完全控制的、受信任的非共享设备填写调查表，并且遵循其他（[在我们的网站上](#)）准则，以保护自己免受在线监控。

HRMI 通过 Qualtrics 收到的调查答复是不记名的。也就是说，我们不会把回复内容和每个调查受访者联系起来。但是，在极少数情况下，某些定性答复有可能可以用来识别某些受访者。因此，我们确定了 3 种不同的数据安全级别，从 1（机密）到 3（公共）。

- **1- 机密：**UGA HRMI 工作人员通过 Qualtrics 接收的初步原始数据，包含所有定性和定量答复。这些数据将在处理后从 Qualtrics 服务器中删除。只有经过安全培训并正在进行相关研究的人员才能有权访问。所有可能识别出受访者的信息都最终将被销毁。
- **2- 研究数据：**用于研究和计算 HRMI 指标的完全去除识别特征的调查答复不需要特殊的安全型，因为数据是完全匿名的。这些数据可以作为复制数据在 HRMI 出版物上在线共享。
- **3- 公开：**汇总数据作为 HRMI 指标发布在 HRMI [人权追踪工具](#)上，并可直接从 HRMI 网站下载。

¹ 为了减轻这种风险，我们提供了潜在调查受访人如何保护自己免受网络监控的[信息](#)。