HRMI

Human Rights Measurement Initiative

HRMI Data Security Policy

HRMI collects two types of sensitive information as part of our Civil and Political Rights metrics development:

- The names and contact details of potential survey respondents.
- Survey responses to our civil and political rights expert survey.

This policy – updated in 2018 following a security audit conducted by a cyber-security firm – explains our security steps for each. As an extra safeguard, we store the two sets of data separately.

1. Names and contact details of potential survey respondents

This information is collected initially from people at our trusted partner organisations, through a secure online form. Additional names and contact details are then sought from our first tranche of survey respondents. Information collected includes the names and contact details (email address and/or WhatsApp or Signal numbers) of potential survey respondents. Key features of our security policy are:

- The secure respondent nomination form is hosted on the HRMI website which has an SSL certificate and is secured by https. This means that the information is secure (encrypted) in-transit.
- The information submitted is sent directly (encrypted) to a dedicated email address hosted by an email service provider - with very strict privacy practices - based in Switzerland.
- Information received is then transferred to our Client Relationship Management (CRM) software. The CRM is certified to all relevant security ISO standards including 27001, 27017 and 27018, which ensures all information in captured, managed and retained in an encrypted fashion. Access to both the dedicated email provider and the CRM is restricted to a small team of New Zealand-based HRMI staff.
- HRMI uses this information to send a link to HRMI's online expert survey to each of these potential survey respondents. The link is typically sent via email (from our dedicated email address), but if requested we can instead send via an encrypted messaging service (e.g. WhatsApp or Signal).

2. Survey responses

The pilot survey is hosted on the Qualtrics website which has an SSL certificate and is secured by https. This means that all information entered and transmitted is encrypted. IP addresses are *not* stored.

The main potential risk to survey respondents is that if their email is hacked or an ISP spies on them, hostile agents may see they are communicating with HRMI and know they are *potentially* contributing to our civil and political rights metrics.[1] But they would not be able to access the survey information submitted itself.

The survey responses that HRMI receives via Qualtrics are unidentified. i.e. we do not link responses to individual survey respondents. However, we have one optional question asking for contact details of other potential survey respondents who we should send the survey to. Also, some of the qualitative responses provided might *potentially* be able to be used to identify some respondents in rare cases. Therefore we have identified 4 different levels of data security from 1 (most secure) to 4 (public).

- Most secure: the initial raw dataset received via Qualtrics by HRMI staff at UGA exists only temporarily (until details of proposed survey respondents are removed and sent (encrypted) to our secure email address – discussed above). These data are deleted from the Qualtrics server at the same time.
- The next most secure dataset (containing both qualitative and quantitative responses) is stored in a separate online secure storage service. Only people who have security training and who are conducting relevant research have access.
- Low security: The dataset of fully de-identified survey responses – to be used in research and to calculate HRMI metrics – requires no special security as the data are effectively anonymous.
- Public: Aggregated data are published on HRMI's website as HRMI metrics. This is what the public sees.

[1] To mitigate this risk, we provide information on how to hide online activity (e.g. by using a VPN, the Tor network, etc).