



Designating a Privacy Officer: Best Practices for Researchers

With the emergence of various privacy laws, researchers must ensure that their companies and organizations (and, to some extent, their clients, contractors and subcontractors) are in compliance with state, federal and international laws, as well as their stated privacy practices. One way companies across the country have been working towards such compliance is the establishment of a designated privacy contact or “privacy officer” position. Titles range from Chief Privacy Officer, to Compliance Officer, Privacy Contact, Director of Privacy, or Privacy Manager.

Why should a research organization or company consider designating a "privacy officer"?

- Various federal (HIPAA) and international (PIPEDA) laws require that covered entities designate a similar privacy-responsible person with their organizations
- It helps establish a rapport with respondents, address their concerns and boost respondent cooperation
- The person in this position helps the firm or organization to limit or avoid legal liability

Think your organization is too small to name a “privacy officer”? Think again!

Many firms with budgetary constraints feel they cannot allocate staff and resources to create and maintain a “privacy officer” position. Depending on the size of the company and amount of private information being collected, the responsibilities of the privacy officer position may not take up the person’s full time. No organization is too small to avoid a lawsuit.

Qualifications for a “privacy officer”:

- Need not be lawyer, but should have familiarity with relevant laws
- Need not be an Information Technology (IT) professional, but should be able to work with IT professionals and know some basic IT terms
- Need not be a researcher, though must have basic understanding of research process and practice
- Need not perform privacy officer functions full-time

The “privacy officer” should also report to the CEO, CIO, CFO or COO, and be a part of (or looped into) business strategy, marketing and sales teams. This reporting structure sends a message to respondents and employees that the research firm places a high priority on privacy concerns. In the alternative, respondents will recognize companies that place the position at the middle or bottom of the chain of command likely place privacy issues at the same level. A strong commitment to privacy is an important key to increased respondent cooperation.

What a “privacy officer” can and should do for you:

- Ensure your organization complies with state, federal and international laws, and professional codes
- Understand and keeps abreast of law/regulation, and educates the rest of organization in that regard
- Keep your organization’s and company’s practices in compliance with your privacy policy
- Help to draft & change privacy policy & practices when necessary
- Advocate for respondents and privacy concerns within the research organization
- Serve as the number one contact (both internal and external) for privacy contentions and concerns
- Serve as a bridge between legal counsel, IT staff, and research personnel
- Position your organization to provide increasingly important privacy related market research consultancy to your clients

More Information

For more information on laws and best practices impacting research, contact MRA, and consider becoming a [member](#) to get free access to the [MRA Compliance Guide](#).