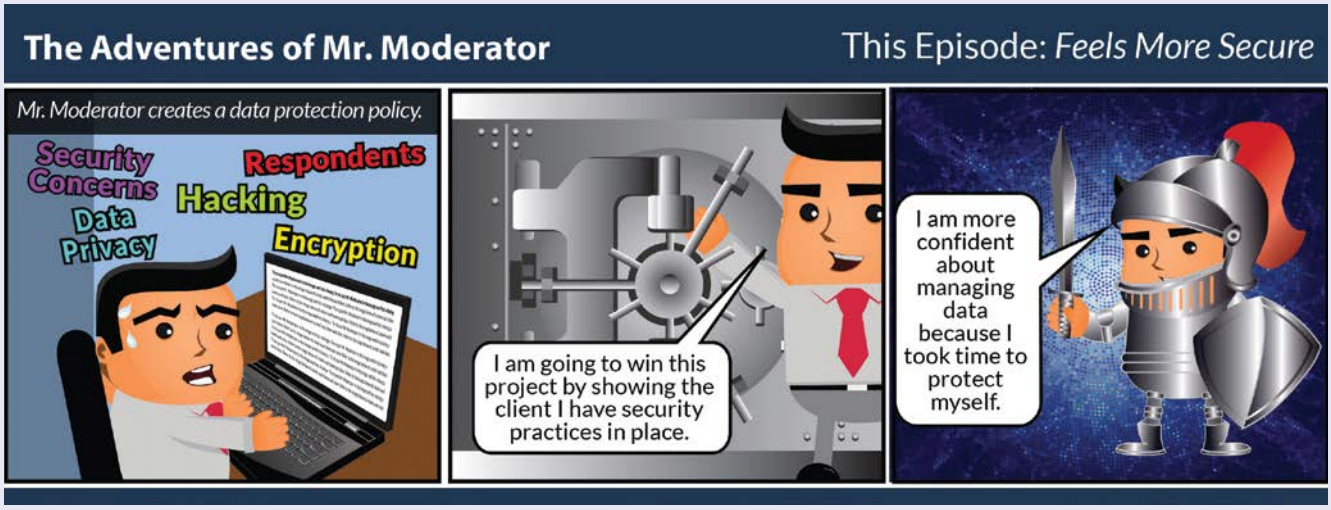
Pause for Protection: Overcoming Roadblocks to Successfully Handling Respondent PII



Life in the early 21st century is hectic. It's hard sometimes to set aside time for those projects you know need to get done. Knowing how to successfully handle respondent PII is one that should not be put off, but the task can be daunting. So we've broken it down into ten of what we hope are more manageable pieces to think about. We hope these will help you.

Strategy 1: Establish a Culture of Accountability

Believe that individuals have substantial rights to manage, correct and control information collected about them and to understand how it is being used. If you have employees, promote an organizational mindset that you are not owners of such data, but rather stewards of that data, and it is your responsibility to protect and safeguard it. Communicate this thinking to the partners you work with.

Strategy 2: Establish and Engage in Best Practices

Address issues of confidentiality before a project begins. Provide respondents with specific detail on the audience for the research. Inform respondents regarding who is the audience for the study results, and how the results will be disseminated. Always have respondents sign an Informed Consent Form. Promote confidentiality by removing identifiers that too closely identify respondents and ask partners to do the same. Review deliverables to make sure identifiers are indeed removed.

Strategy 3: Become More of a Technology Guru

Traditional hierarchical backup approaches aren't enough anymore. Know how to handle data portability to control PII from lost, theft or abuse. Understand what it means to have data encrypted at the source, and avoid transmitting PII over public networks. Use virus software that is sufficiently designed for personal data protection.

Strategy 4: Establish and Enforce a Security Policy

The security in a networked and interfaced world is as weak as its weakest link. Shortcomings in organizations' data privacy and protection technologies can result in data being compromised. Have a technology security policy that covers all critical elements of data privacy and protection, including regular monitoring and auditing, oversight, and appropriate responses in case of a breach.

Strategy 5: Promote and Enforce PII Security and Technology Protocols

Many people typically do not have a full understanding of data flows across their work location. Shortcomings in understanding of data privacy and protection protocols can result in data being compromised. Make sure everyone you work with understands your protocol requirements. If you have employees, have a robust and measurable technology security training program that covers all critical elements of data privacy and protection, enforcement and discipline.

Strategy 6: Understand the Public Mind Set

Individuals value privacy differently depending on the situation. Individuals are least concerned about their privacy when participating in social networking, wikis and blogs—which are often the least secure kind of web interaction. Don't be taken in by these mental gymnastics and conclude that people will not care about their personal data when it is involved in your study. Individuals are wary about the ability of government and businesses to monitor their habits online and combine that information with other personal data to create personal profiles. Research studies fall into that space.

Strategy 7: Engage in Public Compliance

Increase Transparency. Publicly disclose your privacy policy. Require privacy conditions in agreements with subcontractors.

Strategy 8: Become Aware of Non-Compliance Cost

Data breach notification requirements are set to become much tougher. Companies are required to respond to a violation report within 45 days. Top level fines are a percentage of annual global revenue from the preceding year – up to 4%. This is intended so that regardless if you're a Google or a one-person consultancy, violating this law will hurt your business bottom line. Don't let this happen to you.

Strategy 9: Accept that Global Data Privacy Issues Will Be Fluid for a While

Even emerging regulations generally are not sufficiently sophisticated for today's business environment, nor are they consistent or equally applied across industries and countries. Note that there are often separate laws that govern the use of financial and health data.

Strategy 10: Know the Company You Keep

There is a notable difference between organizations' intentions regarding data privacy and how they actually protect it, creating an uneven trust landscape. Understanding the perspective on and approach to data privacy and protection among third parties with whom you do business is crucial. Data must be kept in the safest hands possible, and therefore trust and confidence in your business partners is crucial.

Make sure your business partners know that safeguarding client information is one of your and their most fundamental and important responsibilities, and is essential to maintaining the trust that forms the foundation of client relationships. This is a cornerstone of our approach to working with our clients.

Rebecca West
Global Vice President, Civicom Marketing Research Services