By Rebecca West
- Global VP, Marketing Research Services
- Civicom
- Greenwich, CT
- rebecca.west@civi.com

QRCA VIEWS

APPEARING SOON
IN QRCA VIEWS

PAUSE FOR PROTECTION:

OVERCOMING ROADBLOCKS TO SUCCESSFULLY HANDLING RESPONDENT PRIVACY

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. Just as the woodcutter must take time out from cutting wood to sharpen his axe, you need to take time to do what is necessary to succeed by developing and maintaining respondent data privacy requirements. It is remarkably easy to get into hot and expensive water with a data privacy violation. It's easy to think that because your organization is made up of just yourself or a small group of trusted associates that you don't have to worry so much about data security—that perhaps EU legislation or U.S. data protection guidelines are designed only for the Googles of the world. But that is not the case anymore.

The Potential of Lost Opportunities

Audio and web conferencing changed the opportunity landscape for individual researchers. With the ability to connect globally, independent researchers could compete with large research companies with offices all over the world. That formula has been working well for a decade, and it has helped many QRCs get great projects that previously would not have been obtainable. But now with the changing data privacy requirement landscape, clients are asking more questions and requiring more documentation about

how data protection. This has the potential to turn the tide back to large companies that possess the money to invest in sophisticated privacy assessments to meet complex compliance standards.

Therefore, individuals who are operating independently or as a small business need to take the same necessary steps to protect themselves, both to remain competitive as well as to avoid a data breach fallout. Keeping your data privacy axe sharp is going to help you land that business.

The New Data Regulation Landscape

We live in a global business environment. The U.S. Department of Commerce (DOC) International Trade Administration states that more than 70 percent of the world's purchasing power is located outside of the United States (source at: http://www.trade.gov/cs/factsheet.asp). Whether you already operate globally or even if you do not expect to, you can never tell when the client project coming your way will stipulate cross-border data sharing that requires you to collect, use, and store respondent Personally Identifiable Information (PII).

Transferring data out of the EU is particularly problematic, as the EU has the world's strongest data privacy and protection rules. The deadline for compliance with the EU General Data Protection Regulation (EU GDPR) is May 25, 2018. This consolidated framework will guide business usage of personal data across the EU, replacing the patchwork of existing regulations and frameworks. And don't kid yourself that this will apply to the EU only. The narrative of personal data privacy is rampant in the United States and is likely to get increasing attention, with U.S. companies requiring the same types of compliance and companies putting in procedures for handling all personal data globally.

The risk of non-compliance includes penalties and fines as well as your valuable time and the money you will undoubtedly spend on the legal fees to solve your resulting problem. So what is a researcher to do?

Well, it could be daunting. So let's get started on some solutions.

Strategy 1: Communicate That You Are a "Culture of Accountability"

You most likely believe that individuals have substantial rights to manage, correct and control information collected about them and to understand how it is being used. Incorporate those words into your meetings with clients, into your written proposals, and in important emails. Do you have a website? Make sure this idea is a part of what active and potential clients read about you. If you have employees, promote an organizational mindset that you are stewards of data, and it is your responsibility to protect and safeguard it. Communicate this thinking to the partners you work with.

Strategy 2: Have Both Clients and Respondents Sign Off on Data Use

This sounds easy, but we are all busy. Sharpen the axe. Are you recruiting the respondents for the project? Address this before a project begins. Email your client your understanding of how the research is being used, and get an email back confirming or clarifying. Create a document that each respondent must acknowledge that says the specific detail on the audience for the research and how their data will be used. Have the respondent sign it. An email is easiest. The key is to have a record from the client and a subsequent written and acknowledged record with the respondents that defines the audience for the study results and how the study results will be disseminated. This is to protect you for that future time when a respondent wants to sue you because they say they did not know how the data would be used. And it is also for that time when you really need a record from the client that will transfer this burden away from you because you also have the data's intended use in writing from the client. Don't forget the recruiter in this sign-off loop; every project player must be on the same page.

Strategy 3: Review Deliverables

Did you forward those video files to the client without confirming that no identifiable respondent information is included? The client passes along the video files and suddenly someone from Marketing decides to look up the respondent to ask just a few more questions. This is after he was told he would not be identified, and now he is very unhappy. Suddenly you are being blamed for this. Promote confidentiality by being sure information that too closely identifies respondents is removed and ask partners to do the same. Review deliverables to make sure identifiers are indeed really removed.

Strategy 4: Become More of a Technology Guru

Many people do not have a full understanding of data flows across locations. Understand what it means to have data encrypted both from your computer as well as where you store it. Assiduously

avoid transmitting respondent data over public networks such as hotels and coffee shops. Don't even open data files in these types of places.

Don't ever dial out to respondent phone numbers directly from your mobile device or landline, where those numbers will be stored by your bill provider, most likely online. Have either your valued research facilitator dial out or dial out yourself, in both cases only from an encrypted conferencing bridge which will be the only place that collects and temporarily stores the respondent phone number, rather than dialing out from your own device.

Use antivirus software that is sufficiently designed for personal data protection and keep it up to date. If it slows down your computer too much, it may be time for you to get a new computer—not to disengage the software.

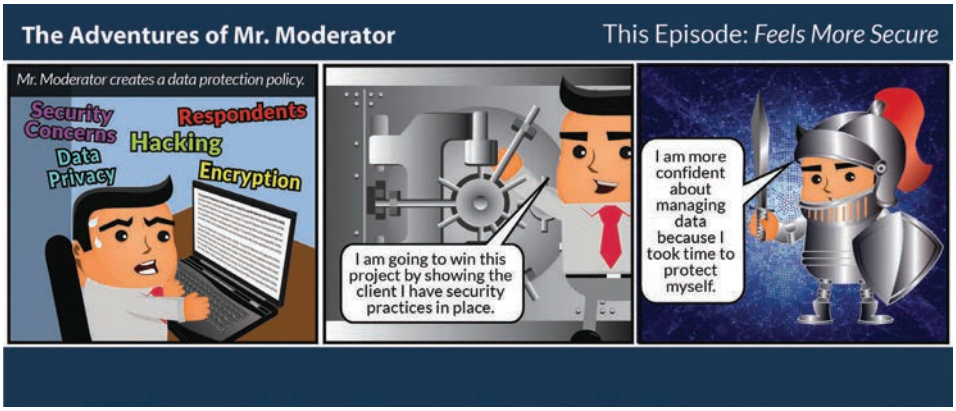
Learn how cloud data protection works. Become familiar with how relocating data from multiple locations to a central repository improves security and reliability.

Strategy 5: Establish and Enforce a Security Policy of Your Own

Think your business is too small to warrant a data security policy? Remember that an important prospect may ask if you have such a policy. You know the large firms have one; you need one too. Prepare a policy in writing that covers the critical elements of data privacy and protection, including your plan for regular self-monitoring and self-auditing and what your responses would be in case of a breach. Keep a copy that you can show in person at meetings. And absolutely have it on your website.

Strategy 6: Promote and Enforce Security and Technology Protocols

The security in a networked and interfaced world is only as good as its weakest link. Make sure everyone you work with understands your protocol requirements. Shortcomings in understanding data privacy and protection protocols can result in data being compromised. In today's world, a simple NDA is not enough. Have all parties sign off on compliance with the items mentioned in Strategy 4. If you have employees, have a measurable technology and data security training program that covers the critical elements of data privacy and protection, enforcement, and discipline.



Strategy 7: Understand the Public Mind-Set

Individuals value privacy differently depending on the situation. People are least concerned about 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 respondents 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.

It may be fun to use Instagram as part of your jewelry retailer study to have people send in photos of the bangles and baubles they plan to wear for the day. It won't be as funny when they sue after they experience a robbery and realize they included photos of the stolen pieces in a research study. Be careful, even when the respondents are not.

Strategy 8: Become Aware of Non-Compliance Costs

Data breach notification requirements are set to become much tougher. Companies—and that means yours, too—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 percent (source at: www.privacyshield.gov). This is designed so that, regardless if you are a huge multinational or a one-person consultancy, violating this law will hurt your business bottom line. Can you afford to pay out 4 percent of your gross revenue for last year, after you have paid legal or arbitration fees and used up your valuable time to address this? Plus, you will have a violation record that will haunt you for the rest of your career.

Strategy 9: Realize that Regulations Are Inconsistent

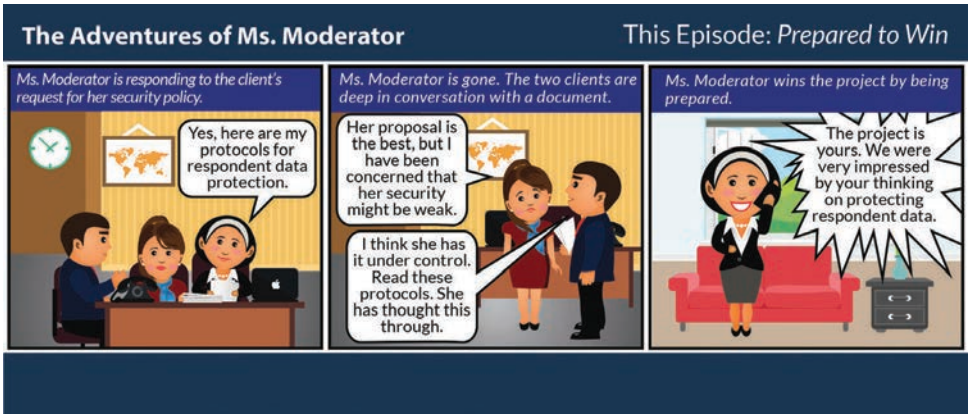
Even emerging regulations generally are not sufficiently sophisticated for today's hack-prone, fiber-optic global business environment, nor are they consistent or equally applied across industries and countries. At my last review, there were something close to 49 different state laws in the U.S. that regulate notification of security breaches, as well as separate laws that govern the use of various types of data such as financial and health data.

It is mind-boggling. Inevitably, you have to go to the lowest common denominator to protect yourself. That means clear documentation on intended data

use, and an understanding that you are best positioned to facilitate communication when you are a conduit between the client, the recruiter, and the respondent.

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 are absolutely 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.



Closing Thought

In summary, start now. Don't push privacy and data protection off your busy plate and wait to do something about it. Make this your year to sharpen your axe of privacy data compliance and win more projects by being better prepared.