



Data Disposal: Best Practices for Survey and Opinion Researchers

A key area for improvement in data security is in the disposal of personal data -- in both electronic and paper formats. “Out of sight, out of mind” is not a tenable or survivable data disposal policy. Personal or client information discarded in the trash or recycling bin is legally and effectively open to anyone. So is any data stored on discarded or donated computer technology, like hard drives and thumb drives, once the devices are thrown away or donated to charity. Electronic data kept beyond its usefulness invites mischief or accidental breach.

Legal requirements for data disposal

Though the law does not apply to most conduct of survey and opinion research, any business or individual who uses a consumer report or information derived from one for a business purpose is subject to the Fair Credit Reporting Act (FCRA) “Disposal Rule”. The Rule requires the proper disposal of information in consumer reports and records to protect against “unauthorized access to or use of the information.”

The standard for the proper disposal of data is flexible, and allows researchers to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

Data disposal best practices

Although the Disposal Rule applies to consumer reports and the information derived from them, MRA encourages anyone who disposes of *any* records containing personal information to take similar protective measures. These measures should be reasonable and appropriate to prevent the unauthorized access to – or use of – such information.

Reasonable measures could include establishing and complying with policies to:

- Burn, pulverize, or shred papers and destroy or erase electronic files or media containing personal data so that the information cannot be read or reconstructed. This includes any items destined for recycling, charity, or some other form of use;
- Only maintain data as long as necessary;
- Audit your organization’s data holdings on a regular basis and keep track of what data is disposed when – and how;
- Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as personal data.

Due diligence could include:

- Reviewing an independent audit of a disposal company’s operations and/or its legal compliance;
- Obtaining information about the disposal company from several references;
- Requiring that the disposal company be certified by a recognized trade association;
- Reviewing and evaluating the disposal company’s information security policies or procedures.

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](#).