COMPREHENSIVE GUIDE:

DATA PRIVACY FOR MARKET RESEARCHERS

CiviCom®
MARKETING RESEARCH SERVICES

TABLE OF CONTENTS

INTRODUCTION

Digitalization has preempted various data privacy laws to appear as the risks of sharing information became clearer. Although data privacy has always been important, more and more information is being shared online, giving it a greater significance. These risks such as data breaches could put client data at risk and damage an organization's reputation.

Moreover, organizations that purposefully gather and manipulate data so they can implement shady marketing tactics exist. For example, this information can be used by phishing scammers who may send emails that contain valid information to individuals in an attempt to gain their trust. As a result, they might share more of their private information such as passwords or click a link that contains malware. To combat this, multiple privacy laws were implemented with the goal to ensure that individuals are given the rights of action over their personal information.

Data privacy plays an even more important role in market research as they deal with personal information on a regular basis. Currently, governments are responding to the modern-day issues of portability and abuse of information so it is important for individuals to protect their rights as well as for researchers and businesses to avoid the penalties of non-compliance. In this guide, the different privacy laws will be discussed along with the costs of violating them. Furthermore, it will explain what measures to take to maintain compliance in market research.

What are the Different Privacy Laws?

GDPR

The General Data Protection Regulation (GDPR) is designed to protect the personally identifiable information and privacy of individuals residing within Europe. The legislation was a reaction to the non-transparency and abuse of information that began with a European citizen's private legal action against Facebook. The EU citizen was surprised to know that Facebook had saved a massive amount of his personal data, even saving every private message he has ever sent. In return, he challenged the tech giant and won.

The GDPR was first introduced on April 14, 2016 and was implemented on May 25, 2018, in order to allow Member State countries to prepare. Since EU Regulations must be enacted into law by Member State governments, the United Kingdom amended its Data Protection Act to comply with the GDPR.

The GDPR aims to give EU citizens full control over their Personal Data and ensure that organizations will properly handle said data. It not only affects organizations in the EU but also organizations in other locations that offer goods and services to citizens residing in Europe.

This can be found under Article 3 which describes the legislation's scope of law. It states that the regulation will apply as long as the personal data of a Data Subject is being processed. This applies whether the processing takes place in the EU or not.

Organizations that are not GDPR compliant may face fines up to 4% of their annual turnover or €20 million (whichever is greater).

Rest assured, a warning will be given upon first non-compliance and will only result in large fines after continuous violations.

What is considered as Personal Data under GDPR?

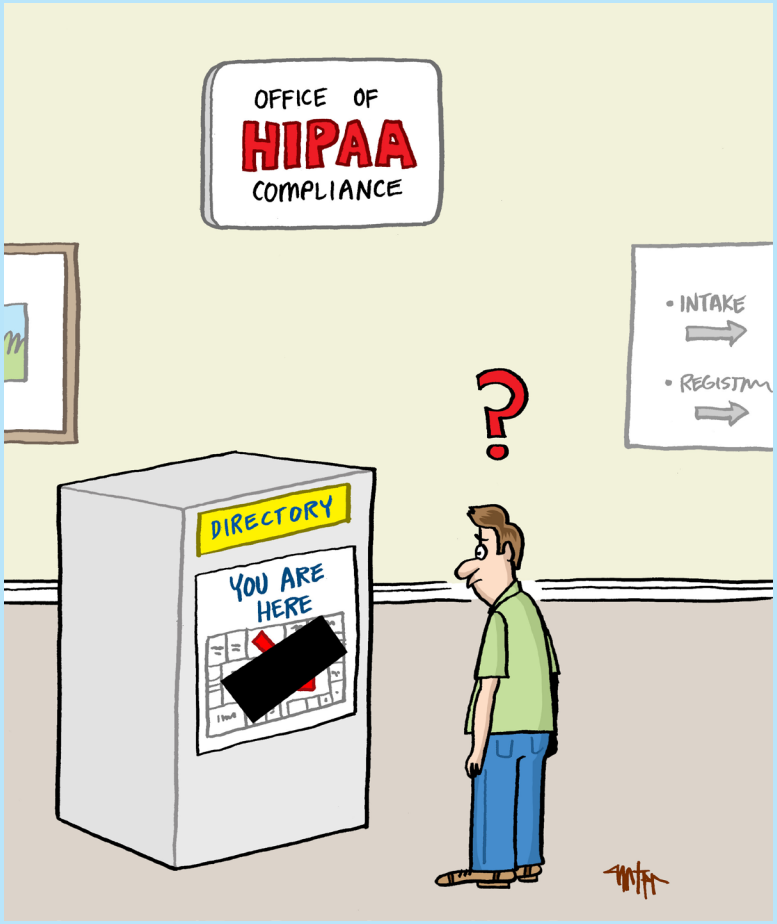
This is any piece of information that can be used to identify an individual or group. Here are some examples:

• Names (first, last, middle, maiden, etc.)	• Audio/visual recordings of an individual
• Dates of birth	• Ban details
• Telephone numbers	• Opinions
• Addresses	• Passport numbers
• Photographs	• Location data

Other special types of sensitive personal data are identified under “special categories”. A breach of this data type carries a high risk of abuse of information for an individual or group which is why it requires a higher standard of protection. Examples of these include:

• Race or ethnicity	• Biological/genetic data
• Dates of birth	• Medical data
• Political or philosophical leanings	• Sexuality/gender identity
• Trade union alliances	

HIPAA



The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that contains security and privacy provisions to safeguard the Protected Health Information (PHI) of patients and research participants. The law dates back to 1996 and was supplemented by the HITECH Act and other amendments to further protect privacy rights and address technological advances.

What falls under the definition of as Protected Health Information (PHI)?

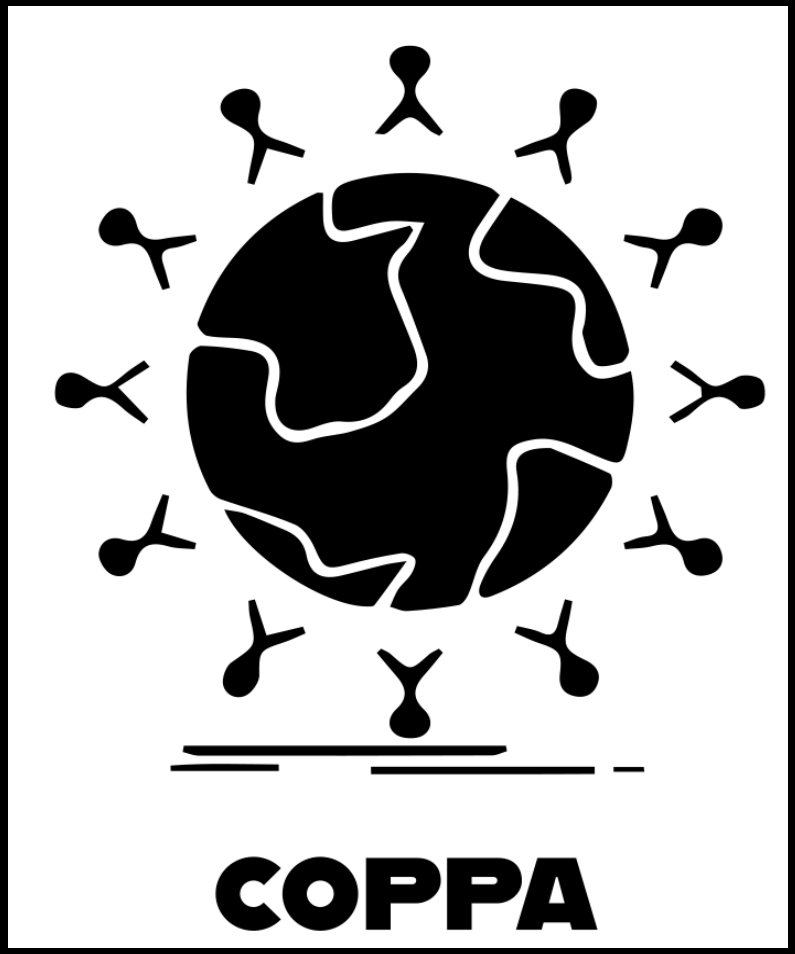
There are 18 identifiers that are considered PHI:

• Names	• Health plan beneficiary numbers
• Dates (Date of birth, admission and release, death, etc.)	• Certificate/license numbers
• Telephone numbers	• Vehicle identifiers and serial numbers including license plates
• Geographic data	• Web URLs
• FAX numbers	• Device identifiers and serial numbers
• Social Security numbers	• Internet protocol addresses
• Email addresses	• Full face photos and comparable images
• Medical record numbers	• Biometric identifiers (i.e. retinal scan,fingerprints)
• Account numbers	• Any unique identifying number or code

A HIPAA violation is non-compliance with any of the security, privacy, or breach notification rules. Here are some of the most common HIPAA violations:

- Looking at healthcare records without authorization
- Lack of adequate employee training
- Lack of HIPAA-Compliant Business Associate Agreements
- Unauthorized disclosures of PHI
- Failure to safeguard PHI
- Improper disposal of PHI
- Failure to report breaches within the prescribed time-frame

COPPA



The Children's Online Privacy Protection Act (COPPA) is a federal law in the United States that aims to ensure the privacy and security of the personal information collected online from people under the age of 13 in the United States. Its main requirement is parental consent before collecting, using, disclosing, tracking, and sharing a minor's personal information. The legislation is enforced by the Federal Trade Commission (FTC).

As for the question, are foreign companies affected by COPPA? The answer would be, yes. As long as the company sells products and services to U.S. citizens under the age of 13, they are subject to FTC regulations.

CalOPPA

The California Online Privacy Protection Act 2003 or CalOPPA regulates data collection, specifically data belonging to California residents. The state law requires commercial website owners to include a conspicuous link to the Privacy Policy on their website.

Under CalOPPA, the following are considered personal information :

- First and last name
- Home and/or business addresses
- Email addresses
- Home and mobile phone numbers
- Social Security numbers
- Geolocation information
- Credit card and other payment details

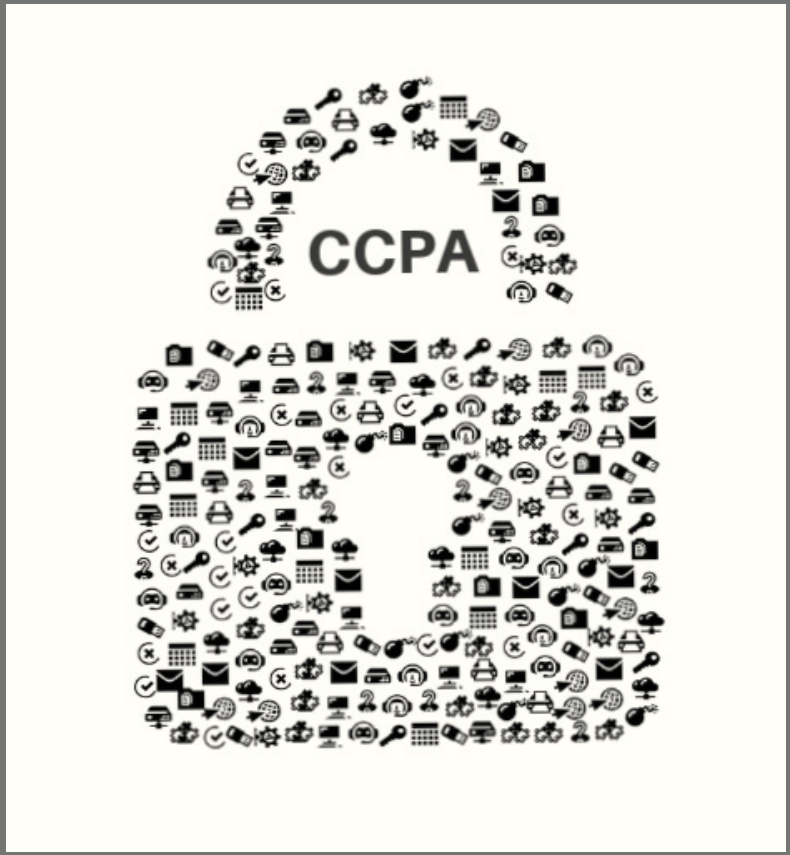
Furthermore, CalOPPA includes a Do Not Track (DNT) disclosure requirement which prevents consumers' online actions to be monitored. The DNT lets the sites know that the user does not want to be tracked.

PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that applies to private-sector organizations in Canada. It requires companies and organizations to obtain an individual's consent before using, collecting and disclosing their personal information.

In April 2018, amendments to PIPEDA were made which was largely motivated by the GDPR. The amendment entitled, "Breach of Security Safeguards Regulations" took effect last November 1, 2018. Among the amendments made are mandatory data breach notifications and mandatory data breach records.

CCPA



The California Consumer Privacy Act (CCPA) was created to further protect the privacy and data of consumers. The CCPA initiative states that the act is intended to "give Californians the who, what, where, when, and how businesses handle consumers' personal information." To be precise, it requires businesses to tell consumers what data it's collecting and gives them the right to opt-out of the sale of their personal information.

The CCPA will be implemented on January 1, 2020, and will be enforced 6 months after that date following the issue of implementation guidelines.

What are the Differences Between GDPR and HIPAA?

The difference between the two lies in their names - GDPR, whose scope is EU citizens, is general, whereas HIPAA, whose scope is Covered Entities and Business Associates in the US., contains the term health information in its name. Since the GDPR contains the word general in its name, it covers more than HIPAA.

Below are other key differences between the two:

1. Consent

Unlike the GDPR where consent must be obtained before disclosing any Personal Data to another party, HIPAA allows covered entities to use of disclose PHI without authorization under these conditions

- PHI can be disclosed to the patient
- Treatment, Payment, and Healthcare Operations
- Incidental use
- Public interest and benefit activities
- Limited data set

However, both privacy policies have similar applications for marketing and communications. GDPR requires organizations to ask for the individual's consent before reaching out to them via phone, email, or direct mail. Sending advertisements or any marketing material without consent is a GDPR violation. As for HIPAA, any patient information used in a marketing campaign must be authorized by the patient ahead of time.

2. Right to be forgotten

One of the individual rights in GDPR includes the "right to be forgotten" where data subjects can request for an organization to delete their personal information under certain circumstances (i.e. if the processing is no longer necessary if it is outside the purposes given for consent (transparency) etc.). On the other hand, HIPAA does not enforce this individual right as it is designed to support the portability of Electronic Health Records.

3. Data Breaches

GDPR and HIPAA have different definitions of breach. HIPAA defines breach as "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information."

Meanwhile, GDPR defines "personal data breach" in their regulation's definitions (found in Article 4) as such:

> *"Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

The biggest difference in data breach between the two lies in the type of data they protect. HIPAA is only concerned with PHI whereas GDPR is concerned with personal data as a whole.

According to the HIPAA Breach Notification Rule, in cases where a data breach has occurred, covered entities must notify the affected individuals, the Secretary, and in some cases, the media.

In cases of data breach that affected less than 500 people, the Office for Civil Rights (OCR) of the Department of Health and Human Services along with the affected individuals must be notified by the final day of reporting each year which is March 1 of the following year.

For breaches that affect more than 500 people, the affected department's OCR and the individuals involved must be notified within 60 days.

In contrast, as stated in Article 33 of GDPR, data breaches must be reported within 72 hours to the competent supervisory authority of the Member State. The notification must include a description of the data breach's nature, the data protection officer's name and contact details, the likely consequences of the personal data breach, and the measures taken to address the personal data breach.

How Do These Privacy Laws Affect The Market Research Industry?

Since market research is now more global than local, many market researchers struggle to comply with various privacy laws.

Email marketing managers and marketing automation specialists are also considerably affected: email marketing managers are now required to ask for consent and make sure that individuals are well-aware of how the organization will use their information. These regulations also restrict email marketers to automatically add these subjects to an email distribution list.

As for marketing automation specialists, they have to ensure that all of the email addresses in their automation system were given with consent. GDPR requires marketing emails to clearly state the company and that is an ad. There should be no misleading subject lines or click bait.

Although GDPR and HIPAA may seem to create limits on market research, they do provide some advantages especially when constructing a targeted campaign. For example, after being granted consent, organizations can gain insight into each individual's interests by exploiting the need for transparency by asking specific questions that will inform them of the types of information that these individuals want and are interested to receive. These privacy policies also provide transparency which can strengthen trust among market researchers, clients, and respondents.

What are the Costs of Non-Compliance?

1. GDPR

As described in Article 83, violations can lead to two types of fines.

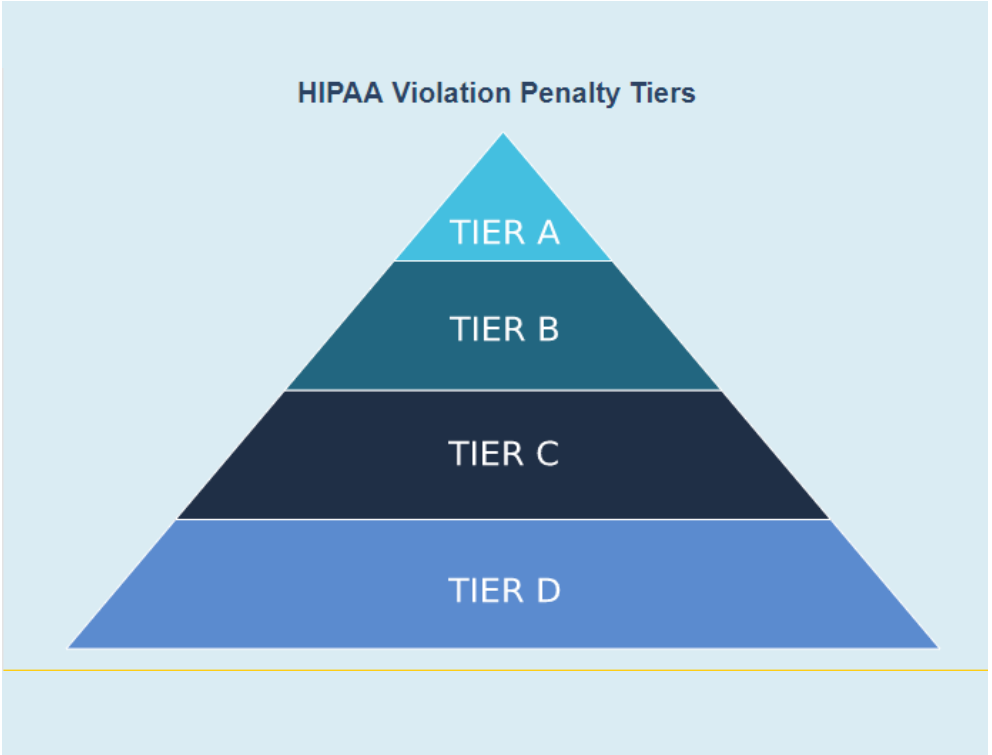
Violations issued with the first type of fine:	Violations issued with the second type of fine:
Insufficient evidence of adequate security	Infringement of Data Subject rights
Neglecting to appoint a Data Protection Officer	Transfer of personal data to a recipient in a third country or an international organization
Not entering into Data Processor Agreements (under what circumstances, these aren't always required).	Non-compliance with an order by a supervisory authority

The first type can incur a fine of up to 2% of the company's annual turnover, or €10 million, whichever is higher; while the second type can incur heavier fines of up to 4% of the company's annual turnover, or €20 million, whichever is higher

The potential costs are not only the fines - there are operational impacts of investigations, loss of business and reputation, breach of contract with clients and individual or class actions for infringing Data Subject rights.

2. HIPAA

The penalties and fines for HIPAA non-compliance are based on the severity of each violation. A penalty can range from $100 to $50,000 per violation, and a maximum penalty of $ 1.5 million per year of violations of an identical provision. The OCR of the Department of Health and Human Services takes into account several factors and uses a four-tiered approach to determine the appropriate financial penalty.



First Tier:	**$100 - $50,000 per incident up to $1.5 million**
Second Tier:	**$1,000 - $50,000 per incident up to $1.5 million**
Third Tier:	**$10,000 - $50,000 per incident up to $1.5 million**
Four Tier:	**$50,000 per incident up to $1.5 million**

3. COPPA

Violating COPPA carries a penalty up to $40,000 per violation and may increase depending on the case specifics. For example, if a company collected the personal information online of five children below 13, it can lead to a penalty of over $200,000.

4. CalOPPA

According to the California Unfair Competition Law (UCL), violations of CalOPPA can lead to a penalty of up to $2,500 per violation. This may not seem much but take note that an organization will receive one violation every time someone visits their website or application if it lacks a conspicuous link or is deemed non-compliant.

6. CCPA

The penalties and fines for CCPA are based on whether the violation is intentional or not. An intentional violation has a penalty of up to $7,500 per record whereas an unintentional violation can lead to fines of up to $2,500 per violation. In addition, it also gives individuals the right to file private actions.

5. PIPEDA

Organizations that are found violating PIPEDA can be fined up to $100,000 per violation.

How to Maintain Compliance in Market Research

It's important to be up to date with the latest data privacy laws, market researchers must know what requirements to address to ensure they stay compliant with every privacy law applicable to them or the data they handle.

The most important strategies to meet these requirements include:

- Consent Management
- Data Minimization
- Data Transfer Security
- Physical Security
- Employee Security Awareness and Training Programs

Most if not all data privacy laws state that before collecting any personal information, obtaining the data subject's consent is a must. When obtaining consent, make sure that it was given voluntarily and can be withdrawn anytime.

Market researchers must also inform data subjects of the following:

- the purpose of the data collection;
- where the personal data will be stored;
- the specific data to be collected;
- the company, organization, data controller's name, address, and contact information
- whether data will be disclosed to third parties

It is also important to manage do not contact and opt-out lists - CCPA does not require consent to sale of information but does require opt-out button on website homepage.

Market researchers must also inform data subjects of the following:

Minimizing the data needed for a project is good practice, as this can reduce the risk of processing beyond a stated purpose, breach, and unauthorized access or disclosure.

Maintaining controls and conducting regular audits and privacy impact assessments can help in ensuring data security.

Here are some questions to ask to help ease the process:

- Are all personal information accurate, complete, and up-to-date?
- Are there existing security protocols against risks such as loss, data breaches, etc.?
- Are there policies put in place to ensure physical security?
- Are there proper procedures for the use and disclosure of personal data?
- Are employees aware and properly trained to implement these procedures?

Since market researchers generally handle various participant data and information, it's essential that they understand the importance of data privacy laws. They must learn how to maintain compliance with data privacy laws and what guidelines to take to protect the organization's reputation and maintain their clients' trust. Moreover, these requirements will not only benefit clients but it also serves as a safeguard for companies and the data they handle. As mentioned, these privacy policies will provide transparency which strengthens trust among market researchers, clients, and respondents.

Non-compliance can greatly put organizations at risk. Not only does this lead to multiple fines and penalties but it also impacts the company's reputation which results to a loss in business. These guidelines can prevent this from happening and will give the measures to take to maintain compliance with data privacy laws.

Civicom has safeguards in place in compliance with
GDPR, HIPAA, and associated regulations.
Connect with us and let's get started with your project.

CiviCom®
MARKETING RESEARCH SERVICES

https://www.civicommrs.com/ 1-203-413-2423 |
inquire@civicommrs.com