WHICH MARKETING DATA PRIVACY LAWS AFFECT FINTECH?

The financial technology market is facing a wave of change and growth. With the rise of new wealthetech trends, it's no wonder the industry is progressing so rapidly. As more financial services and advisors adjust to new data and technology, so are regulations.

California's recent Consumer Privacy Act (CCPA) has driven many other states to follow suit. It's now more important than ever for financial advisors and professionals to educate themselves about cybersecurity concerns as well as which marketing data privacy laws specifically affect fintech.

FINTECH AND DATA PRIVACY

It seems like every day there's news of yet another big-name company leaking consumer data. With more financial applications and digital tools being used than ever before, there is some reason to worry.

A recent report found that two out of five (41%) of U.S. banking consumers already use a fintech app. Of those users, 34% were extremely concerned about their privacy. This doesn't just apply to financial information, but also marketing data. Consumer information like name, age, address, email, and so on are at risk, and new legislation aims to change this.

The good news is that most fintech applications and technology are more secure than users know. New tools like blockchain and AI only make this software safer for user's information. However, anyone involved in the new age of fintech needs to take a close look at marketing data laws to understand which affect their products and services.

GENERAL DATA PROTECTION REGULATION (GDPR)

One of the most well-known (and misunderstood) data privacy laws related to marketing is GDPR. This took effect in 2018, and it's been making waves ever since.

This law specifically applies to anyone within the European Union, but any company that conducts business with consumers in the EU is also held to these standards.

- All collected marketing data must be anonymous
- Data can only be collected with consent
- Data breach notifications are mandatory
- Safely transfer data across borders

CAN-SPAM ACT

If you use email marketing as part of your business, pay attention. The CAN-SPAM Act is a U.S. law that sets rules for commercial email messages. This isn't just for bulk messages, but any type of commercial, promotional email content.

- Don't falsify or mislead with your email header
- Identify any sponsored message as an ad
- Include a valid postal address

- Let users know how to opt-out of future emails

PRIVACY POLICY

All websites and applications need to have a privacy policy if they collect ANY information from users. A privacy policy outlines how the company or website uses personal information or data.

Privacy policies should be clear and easy to understand. If your website or application uses any third-party plugins or services, you'll need to include their privacy information as well.

- How user data is used for marketing or analytics purposes
- What data is collected from users
- Any third-party integrations
- Industry-specific requirements (Fair Credit Reporting Act, Computer Security Act, etc.)

CALIFORNIA ONLINE PRIVACY ACT (CALOPPA)

California is the first state in the nation to set clear, specific requirements for marketing data protection. These regulations apply to any person or business that operates a commercial website or application marketing to consumers in California.

- The privacy policy must be shown on the website homepage or linked on every page of the website
- Describe how the website or application uses consumer data
- Share contact information or a way for users to opt-out of data collection
- Include the effective date of the privacy policy

THE FUTURE OF MARKETING DATA SECURITY

There's no slowing down the growth of fintech, but new regulations are keeping companies accountable. As more and more countries and states take action to protect consumers when it comes to marketing data, the internet becomes a safer place.

In regards to these marketing data regulations above, the biggest takeaway is that transparency is always best. Staying clear with your users about how you use marketing data is always a good idea. From there, keep consumers' best interests in mind and consider security a top priority.