Email Compliance Tips to Avoid Penalties and Preserve Goodwill

Email remains an essential tool for business communication. Workers use it to connect with vendors and colleagues. And email marketing presents a cost-effective way to stretch advertising dollars and strengthen customer relationships. However, to avoid penalties and preserve customer goodwill, organizations must ensure email compliance.

Companies should be aware of several laws affecting email. For instance, the CAN-SPAM act regulates marketing emails in the United States, with even stiffer laws in Canada. The FTC will levy costly fines and penalties against companies who violate CAN-SPAM.

In addition to CAN-SPAM, a growing number of states have begun implementing privacy laws that govern the use of personal data. And industry-specific laws such as HIPAA and PCI DSS mandate data retention and other processes to protect sensitive information.

Stay On the Right Side of Email Marketing Laws

To ensure that marketing emails reach their target audience, businesses and nonprofits must take steps to ensure email compliance. Not only does noncompliance invite penalties, but email filters will send offending emails to the spam box. This will harm your business reputation and negatively affect future email campaigns.

In general, the following guidelines will help you achieve compliance and more effectively reach your target audience.

- **Get permission first** – Never send unsolicited emails. Privacy laws increasingly mandate that companies secure permission before sending marketing emails. Many organizations include an opt-in checkbox on their websites or when users create an account. Do not make the opt-in checkbox automatically checked.
- **Make it easy to unsubscribe** – Every marketing email should include an unsubscribe option, typically a link in the footer of the email. Be sure to honor those unsubscribe requests within 10 days.

- **Avoid misleading subject lines** – Make sure that the subject line directly relates to the content of the email. Additionally, to help keep your emails out of the spam folder, avoid excessive capital letters, suspicious trigger words, dollar signs and exclamation points.
- **Include accurate sender information** – Make sure that the display name next to the sender email address clearly specifies the person or business sending the email.
- **Specify a valid physical address** – The FTC mandates that business emails must include a physical address or PO box.
- **Link to your privacy policy** – Include a privacy policy on your company website and add a link to that policy to your commercial emails. This should state how you will collect, process and store user information, as well as what you plan to do with the information and who else will have access to it.

Email Retention and Data Security Requirements

In addition to email marketing guidelines, regulations also govern email retention and mandate the protection of sensitive information. Email retention laws differ widely from one industry to another, with retention periods varying from one to seven years.

Several industries also impose stringent requirements around securing personal and financial data. For instance, HIPAA requires healthcare providers and their business associates to take extreme care with protected health information (PHI). This includes using proper third-party encryption for all PHI passed through email.

Similarly, PCI DSS imposes strict controls around credit card data. PCI DSS does allow the emailing of encrypted credit card information. However, encryption alone may not ensure regulatory compliance.

Elements of an Effective Email Policy

To ensure email compliance, organizations should implement comprehensive electronic communications policies, or ePolicies. These policies include both written guidelines and the technology that enforces those policies. Periodic training, supplemented by visual reminders, will help users remember and apply the guidelines.

An effective ePolicy will include retention guidelines, as well as rules for when and how data must be encrypted. They may also define rules prohibiting the inappropriate sharing of sensitive information, such as financial data.

Use Technology to Ease the Path to Email Compliance

Organizations cannot afford to leave compliance up to the end user. Compliance technology facilitates compliance by automating processes, adapting to evolving regulations and monitoring for compliance violations.

For example, a quality email archiving solution will automate retention policies. This ensures that archiving and disposal of emails happens according to regulation and without user intervention. Additionally, tight security controls guard against data corruption and editing, achieving the tamper-proof archive mandated by law.

To protect sensitive data, solutions like Microsoft Purview allow organizations to label sensitive data to ensure against improper sharing or deletion. Using AI, the system can automatically apply labels, easing the path to compliance at scale.

To learn more about compliance technology, email archiving or ePolicies, contact the email and compliance experts at Messaging Architects.