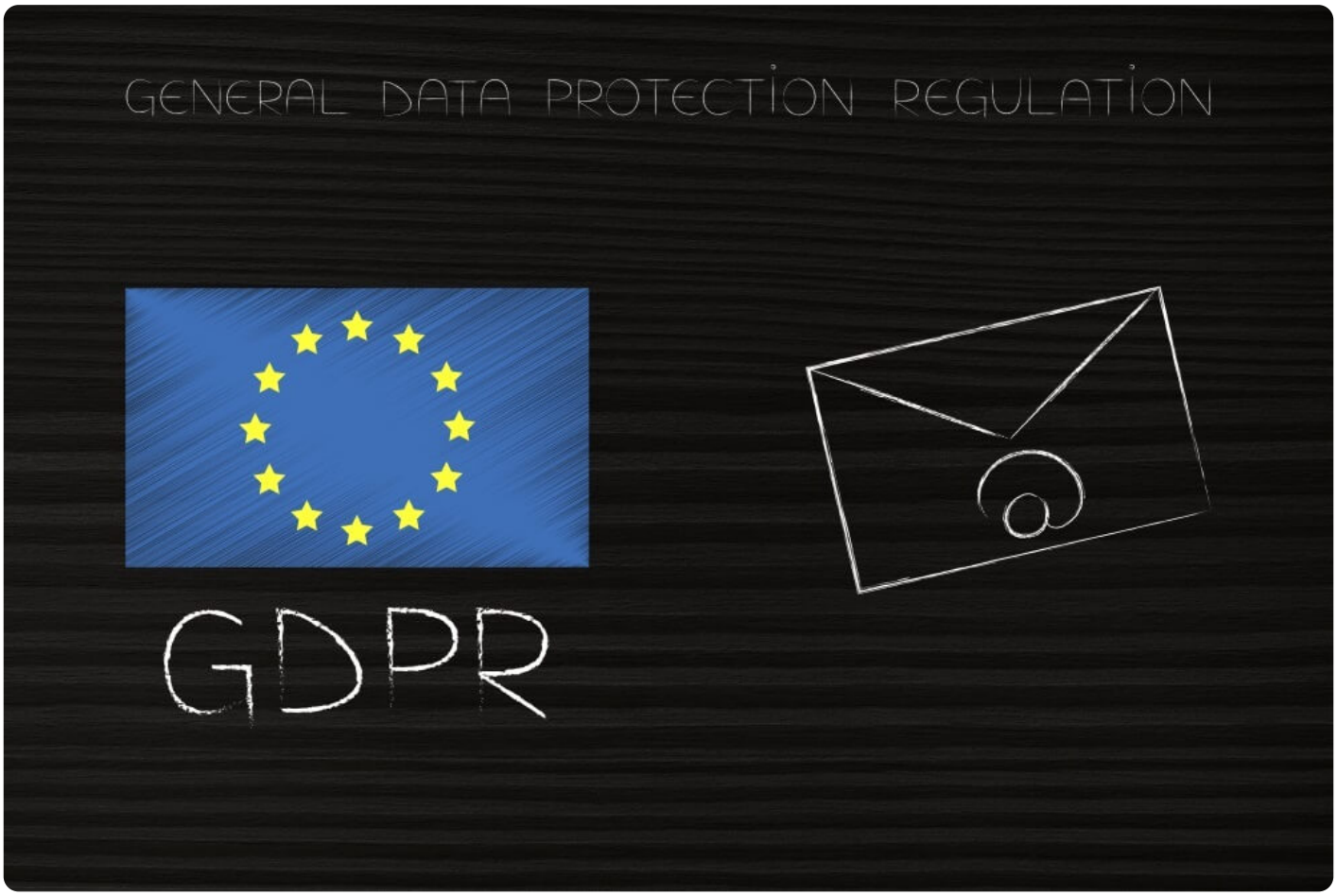
GDPR and Email Marketing: Everything You Need to Know

Posted on October 14, 2021

In the modern marketplace, business leaders must work hard to reach new customers and stay in touch with existing ones at all times. Creating email lists and verifying them is often a cost-effective and reliable way to boost marketing efforts. But of course, when executing a marketing campaign, no business owner wants to run afoul of the law. The General Data Protection Regulation (GDPR) is critical to consider. But with all the noise surrounding business, marketing, and law, one may wonder how the GDPR affects email marketing and email lists.

Before we can answer that question, we first need to learn more about the GDPR.



What Is the GDPR?

We can't deny how much the world has gone digital, where individuals who wish to engage in transactions with organizations (buy products from e-commerce sites, subscribe to various services, etc.) need to provide their personal information in exchange. Sometimes, businesses acquire information from third parties without asking permission from their actual owners. And as many already know, personally identifiable information (PII), such as that collected from consumers, can be sensitive. It's only natural, therefore, for consumers to expect businesses to take steps to safeguard their private data.

In 1995, the European Union (EU) implemented the Data Protection Directive. While this directive created a framework for companies that correspond with consumers via email, it didn't do much to

deter misconduct. The GDPR changed that on 25 May 2018. The GDPR is the EU's solution to protect its citizens' privacy amid the rise in data breaches committed (knowingly or otherwise) by major corporations and fraudulent activity by marketers.

If your organization does business with any EU member country and buys email marketing lists, you must comply with the GDPR because if you don't, you may face significant fines and other penalties.

How Does the GDPR Affect Email Marketing?

The answer to this question is simple. All businesses that use email lists for their marketing efforts must comply with the GDPR, assuming they do business in the EU or with EU member countries. Essentially, consumers must give their consent for virtually everything related to their email addresses. When an organization collects email information initially, it must validate the email addresses and make sure that their owners are informed of and consent to the collection.

Adhering to the GDPR affects several email marketing components, three of which are discussed in greater detail below, along with how exactly they are impacted by the law's mandates.

Privacy Policy

Educating consumers and obtaining consent is trickier than it sounds. Gone are the days when companies could hide policies in long blocks of legalese. The GDPR mandates that businesses must use clean and understandable language to inform consumers through their privacy policy.

All companies must include the following information using simple terms in their privacy policies if they are to fulfill the GDPR requirements:

- **Introduction:** Briefly describe who your company is and what your privacy policy is.
- **Definitions:** If you can't avoid using legalese that may be hard for all to understand, include a section that defines these terms.
- **Personal data processing principles:** Include how your company will abide in terms of

lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality.

- **Personal data types you process:** State all kinds of data you collect and why you gathered the information.
- **How personal data is processed:** Tell consumers what you do with their data and how you handle the information.
- **Personal data retention:** Inform consumers how long you will store their data. Most often, that corresponds to how long your subscription or contract with them lasts.
- **Who the data is shared with:** Companies are allowed to share personal data with suppliers and partners as long as they remain transparent and have a valid legal basis for doing so.
- **International transfers of personal data:** If you must move data from one place to another, from your headquarters to a datacenter, for example, you must inform the information owners.
- **Data rights:** Every company must uphold the eight rights of data owners—right to be informed, right of access, right to rectification, right to erasure or right to be forgotten, right to restrict processing, right to data portability, right to object, and rights related to automated decision-making. Not all of these may apply to every organization, however. Some companies, for example, may have a single office and store data on their premises. In such cases, the right to data portability may not apply to them.
- **Privacy policy changes:** All consumers should be informed of privacy policy changes and why these were made.

Privacy policies must be accessible to all consumers (existing and potential alike). Creating a privacy policy that meets the requirements of the GDPR may not be easy for some organizations. For that, they may need a template. They can download such a guide in various formats, such as a PDF or a document file (Word or Google Docs).

Incentive Drawings

When collecting email addresses, businesses frequently use fishbowl-style drawings. This approach is commonly done in business-to-business (B2B) events and trade shows. When attendees visit a booth, they drop their business cards into fishbowls in exchange for incentives (a month's subscription free of charge, a gift, etc.). Marketers use this information to create lists that their companies can use to increase revenue and profit.

With the GDPR, business leaders must rethink these drawings in a couple of ways. First, they must make all entrants eligible for prizes. More importantly, though, they must obtain informed consent prior to marketing to those who left their contact information behind.

Unsubscribing

Another important facet that the GDPR addresses is unsubscribing from email marketing lists. Businesses must give consumers a convenient and understandable option for leaving such lists. Marketers must also be careful with passing on email lists. Anytime organizations share contact information, they must inform their consumers and obtain specific consent. That is true even if the company is only sharing the information with a subsidiary or parent or sibling organization.

E-Commerce Customers Must Opt In

Any EU citizen that ends up on your mailing list must voluntarily opt in to join. That does away with being able to automatically add someone to your mailing list even if he/she purchases from your website. You can send emails specific to the purchase, such as a receipt, but not for anything else. Email verification is required at all times.

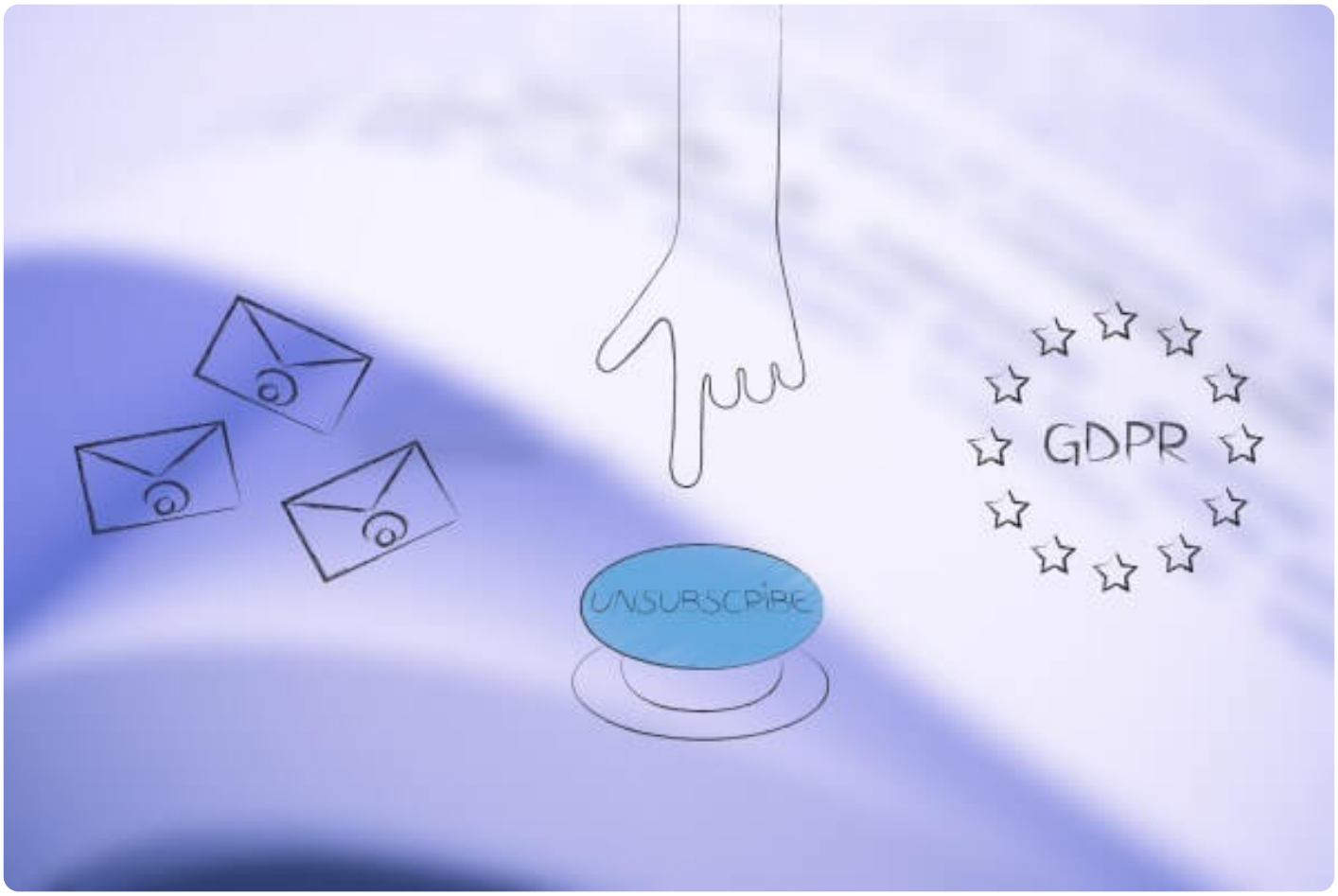
No Pre-Checked Boxes

Any business that runs an e-commerce store with pre-checked boxes for customers to opt in to

newsletters and marketing emails on their checkout pages is not allowed to do that anymore. Customers must instead be presented with empty boxes that they can tick if they want to receive emails from you.

Adding Contacts to Lists

Keeping with the theme of email verification to comply with the GDPR, people must give you direct permission to be added to your contact list even if they already signed up for another service with you before. For example, if customers sign up to receive your free e-book, that's the end of your relationship unless they agree to sign up to receive further communications from you via email.



Why Is Email Verification Important for GDPR Compliance?

The email verification procedures under the GDPR may seem like a roadblock. But in reality, it can be a great opportunity to filter those who don't want to hear from you in the first place, increase your email open rates, and improve your engagement numbers.

The GDPR requires companies to collect consent for email addresses that are "freely given, specific, informed, and unambiguous." If companies want to remain compliant, they need to run re-permission campaigns to check if their existing subscribers' consent is compliant with GDPR. Here's where email verification comes in.

Before running re-permission campaigns, marketers need to validate and clean their email lists to detect mailboxes that may have been deleted, domains that don't accept emails anymore, or invalid email addresses—i.e., those that don't adhere to the prescribed Internet Engineering Task Force (IETF) format. This can be done automatically using email verification tools such as Email Verification API or Bulk Email Verification API.

Once email lists are validated, the goal of the re-permission campaign is to remove those email addresses whose owners may not be willing to receive messages from them. That's what the GDPR wishes to do, too, albeit only for EU citizens. In a sense, email verification and GDPR compliance work hand in hand, so organizations don't suffer the consequences of GDPR noncompliance.

Companies that run afoul of the GDPR face significant monetary penalties. They also often need legal representation throughout investigations. If your organization uses email lists as part of its marketing strategy, you must comply with the GDPR. Fortunately, once you understand the basic framework, you will be able to avoid the unpleasant repercussions.