HOW TO MAKE YOUR NEWSLETTER SUBSCRIPTION

GDPR COMPLIANT

A guide by
Digital Kitchen

digital kitchen

WWW.DIGITALKITCHEN.RO

HELLO@DIGITALKITCHEN.RO

TABLE OF CONTENTS

INTRODUCTION

GDPR is a set of security and privacy laws in the European Union (EU) that regulate how data should be collected and processed.

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The GDPR requirements apply to every company that targets or collects data related to people in the EU.

Contrary to what some marketers expected, the GDPR didn't kill email marketing. Quite the opposite, GDPR-compliant brands have a chance to strengthen their relationships with their audience, build trust, and improve email engagement.

Email marketing has become less disruptive and more relevant and trustworthy. Now, companies think twice before sending a promotional email, and customers no longer see marketing communications as irrelevant and intrusive.

WHAT ARE THE PRINCIPLES OF GDPR?

Lawfulness, fairness, and transparency

When collecting personal data, you should align with three sub-principles of the GDPR:

- **Lawfulness**: You have a good reason to gather the data.
- **Fairness**: You don't withhold information about the reasons behind collecting the data.
- **Transparency**: You're open with data subjects about what your company does and why you need the data.

Users should know where their data goes and how it's processed. You should add this information right within your data collection form.

Purpose limitation

There should be a "specified, explicit, and legitimate purpose" behind data collection. For instance, if you state you need the user's email address to send transactional emails, you aren't allowed to reach them with marketing communications.

The principle of purpose limitation protects individuals from wrongful use of data, spam, and irrelevant communications.

Data minimization

GDPR strives to minimize the collection of excessive data. To comply with this principle, an organization can only ask for the data they need to achieve the stated purpose.

This rule makes it easier for companies to manage data and keep it up-to-date. It also minimizes the damage caused by a potential data breach.

Accuracy

A business must also take responsibility for updating the data and erasing incorrect information whenever they spot it. Individuals have the right to request the removal of irrelevant or incomplete information within 30 days.

For instance, when a user opts out of your marketing communications, the principle of data accuracy requires you to remove their email address from your marketing email list.

Storage limitation

The data collected should be stored only for a specified timeline. If you no longer need the data to achieve the goal you previously established, you must delete it from your database.

You can also archive the data, but you need to indicate the retention period and detail reasons for doing so in your privacy policy.

Integrity and confidentiality

According to the official legal text of EU GDPR, this principle helps to ensure that the data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

You must adopt proper measures to secure your audience data from deliberate attacks or accidental breaches. For email marketers, this means:

- Choosing a reliable email marketing service provider that follows email authorization standards
- Collecting necessary data only
- Using email encryption (your email marketing platform should do this for you)
- Allowing access to customer data only to employees who need it

Accountability

The seventh principle requires you to collect all the necessary documentation that may prove that you meet compliance regulations. This documentation may include:

- Proof that you have obtained user consent before collecting the data
- Purpose of data processing
- Explanation of how the data has been used
- Data retention policy
- Information on security measures implemented

Maintaining records of data processing activities allows you to demonstrate your compliance with GDPR, saving you a lot of trouble.

WHY SHOULD WE COMPLY TO GDPR RULES?

Regardless of what the business spends, it'll be worth it because there's one significant reason to stay GDPR compliant — large fines for non-compliance.

GDPR Fines:

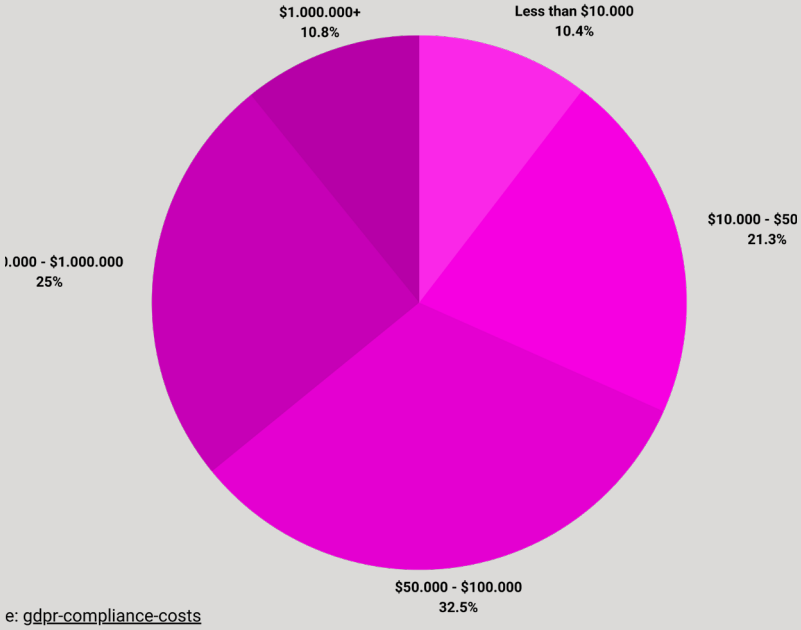
During the first 20 months of GDPR, more than €114 million have been issued in fines. (GDPR.eu) The largest fine for GDPR violations as of 2022 was issued by Luxembourg DPA to Amazon Europe. It was a fine of 746 million Euros. (Statista)

Under the GDPR, fines can reach €20 million or 4% of the company's global turnover for the preceding financial year. The fines are flexible and depend on the severity of the infringement which is determined by the nature, gravity, and duration of the GDPR violation.

The biggest ever fine was registered in July 2021. Amazon was again found incompliant with general data processing principles and had to pay a penalty of €746 million. It's followed by Meta (€405 million), WhatsApp Ireland (€225 million), and Google (€90 million).

But these statistics shouldn't give you the impression that only corporate giants like Google and Facebook are subject to GDPR penalties.

In 2022, over 350 healthcare organizations, restaurants, local service providers, educational centers, stores, and other small businesses were charged for non-compliance with the GDPR. Since 2018, over a thousand companies have been fined, and this number is growing.



e: gdpr-compliance-costs

348

total number of fines by september 2020

€ 490,878,530

the amount of fines by september 2020

EMAIL MARKETING BEST PARCTICES UNDER GDPR & E-PRIVACY DIRECTIVE

GDPR and e-Privacy Directive prohibit organizations from sending direct marketing communications to individuals without first obtaining their consent. Such consent must be freely given, informed, specific, and unambiguous. Typically, organizations obtain consent from individuals by presenting them with a checkbox on their website asking whether they would want to receive marketing emails.

Let's look into some of the best practices of email marketing for organizations aiming to comply with the GDPR and the e-Privacy Directive.

Explicit Opt-In

Organizations must allow individuals to actively confirm their consent by taking affirmative action, such as ticking an unchecked opt-in box. Such a checkbox must not be pre-selected or pre-ticked by default, and the individual must actively select it themselves.

Separate Consent and Terms & Conditions

Organizations must ensure that an individual's consent is specific to the purpose of sending marketing communications. Consent should not be bundled up as a non-negotiable part of the terms and conditions of a service or the organization's privacy policy.

Simplify Consent Withdrawal

Organizations must provide an option to opt-out in every subsequent marketing email to the individual. This may be done by including language at the bottom of the marketing communication that instructs individuals on how they can opt-out.

For example: "If you do not wish to receive further marketing emails from us, please click here".
In addition, the opt-out must be free-of-charge, simple and as easy as giving consent. The next question is what an organization must do when an individual opts out.

- It must not send those individuals any further marketing emails nor contact them to invite them to opt back into marketing,
- It must delete the personal data collected to send marketing emails. However, an organization may suppress personal data only to ensure that those individuals are not sent any more marketing emails unless they opt back in at a later stage,
- Suppression of personal data involves retaining just enough information to ensure that the individual's preferences are respected in the future. An organization must always inform individuals about such suppression so that they may ask it to remove or delete their details entirely,
- Honor the opt-out request promptly and avoid any unnecessary delay.

Soft Opt-In Exception

GDPR and e-Privacy Directive allow organizations to send marketing communications to individuals whose details they obtained in the context of the sale of a product or service i.e. existing customers without making them select an opt-in checkbox. This is referred to as the soft opt-in exception.

However, to rely on a soft opt-in exception and send marketing emails to individuals without their consent, the following conditions should be fulfilled:

- The organization obtained the individual's contact details in the context of the sale of its product or service,
- The individual did not opt-out at the time of providing their personal data, and a clear and distinct opt-out ability was provided to them at the time their details were being collected,
- The organization must send marketing emails only about its products and services and similar products and services for which the individual's details were initially collected,
- The organization must clearly and distinctly remind individuals about their ability to opt-out at every subsequent marketing communication,
- Opt-out should be simple, free-of-charge, both at the time of the collection of the personal data from individuals and in each subsequent marketing communication.

The interpretation of the term "in the context of the sale of a product or service" may differ from one EU member state to another.

LEGAL FACTS

Consent in accordance with Art. 6 Paragraph 1 lit. a) GDPR to receiving the newsletter must be provided through an unambiguous, confirming action, with which the user communicates that he or she consents to the processing of the applicable personal data in a voluntary, informed manner and for the specific case indicated (Recital 32).

The website operator may neither coerce the user to provide consent (e.g. by blocking access to content when the user has refused consent for his/her personal data usage) nor "sneak" a newsletter upon them, otherwise the requirement for the voluntary and informed nature will have been violated (Art. 7 GDPR).

HOW TO CREATE A GDPR-COMPLIANT NEWSLETTER IN 3 STEPS

The goal of every newsletter marketing campaign is clear: to generate as many new subscriptions for the newsletter as possible.

Firstly, we should point out that anyone wishing to do legally compliant newsletter marketing should offer the users as much transparency as possible and, in every case, obtain consent to process their personal data.

Step 1: Ensure the unambiguity of consent

It must be clear to the user that downloading the white paper will automatically result in subscribing to the newsletter. That to which the user is consenting must be clearly recognizable. This means: The user can only be made aware of the purpose of the white paper download and coupling it to a newsletter subscription if consent has been obtained in accordance with data protection law.

A negative example: you go to a restaurant and leave your data due to coronavirus tracking and tracing. A few days later you get mail from that restaurant. However, you didn't consent to receiving marketing or advertising. Feels weird, right? Compliance with purpose limitation (Art. 5 GDPR) in terms of the GDPR definitely does not apply here.

How do I ensure that the user interested in the white paper has explicitly consented to the newsletter subscription?

Unambiguous consent:

Use a separate control field so that the user can provide explicit consent to signing up for a newsletter. The control box may not be pre-activated – it must be actively and manually ticked. This ensures that it's abundantly clear to the user for what purpose (here: newsletter) he or she is giving consent.

Shoring up consent via a double opt-in:

We also recommend solidifying the newsletter sign-up via a so-called double opt-in ("double agreement"). Large mailing providers offer this option as a standard. Here the user receives an email after registration (first opt-in) at the email address provided in which he or she confirms registration via a link (second opt-in).
The advantage for you as a provider: You know directly whether the address provided is correct and

Step 2: Ensure “clean” data processing

Once users have explicitly consented to having their data processed, this must now be done in accordance with the GDPR. Processing can generally be divided up into two areas:

Upon collection:

Process data sparingly: Follow the principal of sparing data use and only collect data which is absolutely necessary for the marketing campaign.

Ensure encrypted transfer: Data transfer must always occur in encrypted form. This is the only way of ensuring that data does not fall into the hands of third parties without permission. Websites use a so-called SSL certificate for this purpose which is recognizable through a URL beginning with “https://” and a padlock symbol in the address bar.
Don’t forget to name and indicate third-party services: Bot queries can be countered by using registration forms with protection systems such as Google’s reCAPTCHA. Here you should make it absolutely clear to your users about the use of third-party services because these also collect data.

After collection:

Save data securely: Once the data has been gathered it must be saved in a safe place and protected from outside attacks (Art. 32 GDPR). The scope of the measures to be taken depends on several factors (identified as “appropriate protection level” in the regulation).

Make revocation easy: Users must be able revoke their consent without great effort to ensure GDPR-compliance. Users must be made aware of this fact before they sign up to the newsletter. To enable a straightforward opt-out, a link should be embedded in every mailing whose activation not only stops the newsletter being sent but also the complete deletion of user data.

Step 3: Establish full transparency

Users have the right to know exactly what happens with their data

.
Integrate data protection provisions: Link the data protection provisions for the newsletter during the opt-in. Make clear to your users which data is being collected and for which purpose, how the data is processed and how they can opt out.

Openly communicate info regarding CRM/mailing providers: A CRM solution is often used, especially with large marketing projects in the B2B and B2C space, to save data sets from the newsletter subscribers in one central location. The users must be made aware that their data is forwarded to third parties. Similar applies for large mailing providers which offer website operators management of addresses via their platform. Users must likewise be informed about the contract data processing.

Our tip: Pay close attention when selecting a mailing/CRM provider to which data protection measures they have adopted and to how subsequent data processing is configured. If in any doubt, decide on the most transparent solution which uses the very least amount of data possible.

CONCLUSION

Most companies have taken significant steps to upgrade their data protection efforts and cybersecurity but there are still those businesses that suffer non-compliance fines from the data protection authorities.

There are two things that are undeniable, though! The first is that customers want to know that their data is not being abused and used in ways they don't expect or understand. And the second -and most important for businesses- is that investing in privacy pays off and doesn't impede business growth. At first glance, the GDPR can be seen as a hindrance for marketing activities, but a closer examination of the regulation reveals that it gives marketers an opportunity to build more transparent and meaningful relationships with their customers.

The GDPR mirrors the DMA's long-held view about the need to place the customer at the heart of everything we do and echoes our commitment to a code that enshrines five key principles which marketers should follow:

- Put your customer first
- Respect privacy and meet your customers' expectations
- Be honest, be fair, be transparent
- Exercise diligence with data
- Take responsibility, be accountable.

Out of the six legal bases for which an organisation can process data of an individual, two closely apply to marketing activities: legitimate Interests, in certain circumstances, and consent.

Consent, the more obvious choice for marketing activity, gives the GDPR its poor reputation in our industry, but the DMA has established vital building blocks within the new regulations that will safeguard the interests of marketers. This has been made possible mainly by our advocacy for direct marketing to be carried out under legitimate interests, thus opening up more opportunities to build and strengthen relationships with customers.

Consciously setting up GDPR-compliant newsletter marketing is not rocket science, but it does require investing some time. A project like this is worth planning in a certain time schedule – and the matter should certainly not be left to the last minute.

GDPR-compliant newsletter marketing lives and dies with transparency – and of course the voluntary, explicit consent of the subscribers. Most importantly, clearly and unambiguously design the consent for newsletter marketing, ensure data security during the processing of data and communicate transparently with the users.