

# GDPR SOS Kit for marketers



# Table of contents

<b>Welcome .....</b>	<b>3</b>
<b>1. High urgency .....</b>	<b>4</b>
1. Clean your newsletter database and conduct re-permission campaigns.....	4
2. Scrutinize your third-party providers.....	5
<b>2. Medium-high urgency.....</b>	<b>6</b>
3. Evaluate your data and lead collection process .....	6
4. Update your Privacy Policy and send an email notification .....	7
<b>3. Medium urgency.....</b>	<b>8</b>
5. Change the internal mindset .....	8
6. The next big step: Get ready for ePrivacy .....	9



# Welcome

**GDPR came into effect in May 2018**, and yet a large number of small-to-medium size companies are still not sure, or not confident, they are GDPR compliant. The penalties for non-compliance are drastic, not to mention the business impacts and consequences, and it's important to **remember that no one is entirely exempt**. Regardless of company size or location, anyone collecting, processing and storing personal data of citizens within Europe needs to be compliant.

As [the first company in the world to have obtained the AFAQ certification from AFNOR Certification](#), which guarantees that Mailjet by Sinch respects the main principles of GDPR, **we know first-hand what it takes** for a marketing department to implement changes to ensure compliance with national and international regulations. We also know that for most marketers, GDPR hasn't been a full-time priority. But if you're still unsure, there are **changes you must definitely make as soon as possible if you haven't already**.

Whether you're **starting from scratch or double checking** that you haven't missed something, the **most important actions** that your marketing department **must do** are contained in this kit, broken down into three categories:

- High urgency
- Medium-high urgency
- Medium urgency

This is provided for informational purposes only. We suggest that you consult a lawyer about your specific obligations under GDPR.



PART 1

# High urgency

## 1. Clean your newsletter database and conduct re-permission campaigns

In order to send any electronic message (email, SMS) to a contact, you must have gained explicit consent and have this well-recorded. The following material will help you document your existing contacts correctly and assess if a re-permission campaign should be considered.



### Steps to take:

- 1.) Document your current subscriber database:
  - What personal data do you already hold?
  - Where did it come from and who have you shared it with?
  - Via which channel and source have you obtained consent?
  - What has the person consented to receive?

The temporary consent of soft opt-in when collecting an individual's email details is not considered as explicit consent or a satisfactory practice. Consent must be asked in unambiguous language.

2.) If you do not have express consent properly documented, a re-permission campaign is normally recommended. But now that the GDPR effective date has passed, any communication without this proper consent could put you at risk. So you can either remove everyone for whom you don't have proof of consent from your email list or send a re-permission campaign at your own risk. This may be combined with a Privacy Policy update email (assuming you have not informed your contacts about this either).

### Tools and readings:

 [Documenting your newsletter database: Template](#)

*A template to document your existing newsletter database. This will help you identify the contacts for whom you do not hold a clear consent record and could therefore include in a re-permission campaign.*

 [How to conduct re-permission email campaign: Template and examples](#)

*Learn more about a re-permission campaign and see examples of ones done by other brands. Download this template in MJML and HTML [here](#).*

## 2. Scrutinize your third-party providers

A highly misunderstood element is where data privacy responsibility starts and stops. To clarify: Once you have collected personal data, you are responsible for ensuring that it's protected, wherever the data may flow. This means that if you share this data with a third-party provider, you are responsible for ensuring that this third-party provider is also GDPR-compliant. If not, you are in breach of GDPR.

Examples of third-party providers with whom data is often shared:

- CRM systems
- Email service providers
- Click-to-chat software
- HR management software



### Steps to take:

You need to vet all third-party companies you work with to understand how the personal data that you have collected for your customers is being protected, and where exactly that data is being shared and transferred. You will then need to record this within a data registry.

### Tools and readings:

 [Third-party provider data registry: Template](#)

*Template to record to which third-party providers your data is flowing and identify risks.*

 [Third-party provider checklist](#)

*Checklist to make sure that your providers are GDPR compliant.*

 [Email service provider checklist](#)

*Checklist of questions to ask your ESP to ensure that they are GDPR-compliant.*



PART 2

# Medium-high urgency

## 3. Evaluate your data and lead collection process

Marketing and sales departments undergo a number of methods to collect customer data. For example, many companies still purchase third-party lists, namely for sales prospecting and marketing purposes. Under GDPR there are six legal bases for processing personal data, and it's important that every data collection method you employ is based on one of these. In marketing and sales departments, consent and legitimate interest are the most common bases.

Examples of common data collection methods:


- Purchasing of third-party lists
- LinkedIn email scraping
- Soft opt-in (i.e. newsletters)
- Forced opt-in (i.e. adding someone to a newsletter list when they've downloaded a guide)
- Referral programs (be careful with "Refer a friend" campaigns)
- Online contests/sweepstakes



### Steps to take:

Some of the above need to be stopped immediately, while, for others, you need to prove which legal basis applies. If it is consent, it is imperative that you know when the consent was obtained (data and time stamp, for example), and the exact purpose for which the consent was given.

### Tools and readings:

 [The right way to ask for consent: Examples](#)

*Best practices on how to ask for consent with a focus on newsletter opt-in.*

[Questions to ask your data vendor: Checklist](#)

*A checklist of critical questions to ask your Data Vendor to ensure that, if you purchase customer information, it's GDPR-compliant.*

## 4. Update your Privacy Policy and send an email notification

Under GDPR, there are certain specifications that need to be applied to your company's Privacy Policy. What's more, it's best-practice to communicate to your customers that this policy has been changed. The following materials will showcase the major updates that need to be made and best practices for how to communicate these updates to your customers.




### Steps to take:

**1.)** Update your Privacy Policy. Under GDPR, here are the certain additions that must be taken into account within a company's Privacy Policy:

- The Privacy Policy must contain the contact details of the Data Protection Officer, where applicable.
- The Privacy Policy must contain the purposes of the processing for which the personal data are intended as well as the legal bases for the processing. Including which of the six legal bases apply is a new addition.

**2.)** Communicate to your users that your Privacy Policy has been updated. This is best practice and is normally conducted by email.

### Tools and readings:

 [Do you need a DPO?](#)

*Insights from Mailjet's own DPO in her GDPR journal.*

 [How to conduct a Privacy Policy email update: Template and Examples](#)

*Learn more about a Privacy Policy email update and see examples of ones done by other brands.*



PART 3

# Medium urgency

## 5. Change the internal mindset

Intent is the most important element that will be scrutinized if a company is brought to court for breaching GDPR. The goal of GDPR is to make companies change their global approach to data protection and, to do this, every department needs to be onboard. Since May 25th 2018, customers have the following rights. Right to be forgotten; be informed; have personal data deleted; have a copy of their personal data (within a month, free of charge);

- Right to data portability – data electronically sent to them in a commonly used readable format;
- Right to restrict automated decisions and profiling;
- Right to object.

Are all of your departments already prepared to handle this?



### Steps to take:

Our study discovered that only 35% of companies had provided team trainings about GDPR before it came into effect. Many still haven't done so several years later. We understand that this task may seem daunting, but these are the most effective ways to ensure that every employee understands the importance of GDPR, the rights consumers have, and the role each person plays in delivering this.

### Tools and readings:

- [How to prepare your company to adopt a GDPR compliant mindset: Checklist](#)

*A checklist of actions to take with different teams across your company to ensure that every employee is informed and can accurately respond to customers regarding the company's GDPR compliance.*





## 6. The next big step: Get ready for ePrivacy

The ePrivacy regulation was originally expected to be implemented at the same time as GDPR and it is also referred to as the “cookie law.” It is a law from the EU Commission designed to strengthen the protection of EU citizens’ private lives and significantly alters the rules on cookies and other online trackers. Once you’ve adopted all the other changes suggested in this GDPR Kit, you’ll have to dive into ePrivacy, as it will also affect your marketing practices.

Back in 2018 we conducted [a study with Morar Consulting](#) and asked marketers how they believed ePrivacy would affect their department and company. The results were significant:

- 91% of marketers expected that the implications of ePrivacy would directly cause a loss in global web traffic.
- 30% planned to reduce the amount of cookie-based display, paid search, and retargeting they carried out.
- 79% of marketers predicted they would use email marketing more as a channel post ePrivacy.


Now, several years later, most of these marketers have seen a change in their marketing practices, with new lead generation methods and retargeting activities in place to comply with the upcoming EU cookie law.




### Steps to take:

[The ePrivacy directive text is not yet finalized](#), but in the meantime, marketers should already analyze their current cookie policy, cookie policy notice, and data collection methods – three items that will be greatly impacted by ePrivacy.

### Tools and readings:

 [ePrivacy: Everything you need to know about the EU Cookie Law](#)

*Learn about ePrivacy and what it will mean to your business in our comprehensive post.*

 [Marketers and ePrivacy: 2018 Research report](#)

*Insights on how marketers believed they would be impacted by ePrivacy and how they would shift strategies following its implementation.*





More than 40,000 companies around the world use Mailjet by Sinch to strengthen connections with customers and subscribers while building their businesses through email marketing. Brands like Microsoft, Kia Motors, and Toast trust Mailjet to send billions of emails every year. Mailjet combines an intuitive, drag-and-drop email campaign builder with easy-to-use deliverability features to help businesses create and send beautiful emails without touching a single line of code.

Founded in Paris in 2010, Mailjet has offices in tech hubs around the globe, including the UK, US, Spain, Germany, and France. Mailjet is proud to be part of **Sinch**, a leading Communication Platform as a Service (CPaaS) provider, offering messaging, voice, and video communication solutions to a large global customer base. Mailjet is both ISO 27001 certified and GDPR compliant, offering its clients the highest levels of data security and privacy.

For more information, please visit [mailjet.com](https://mailjet.com).

