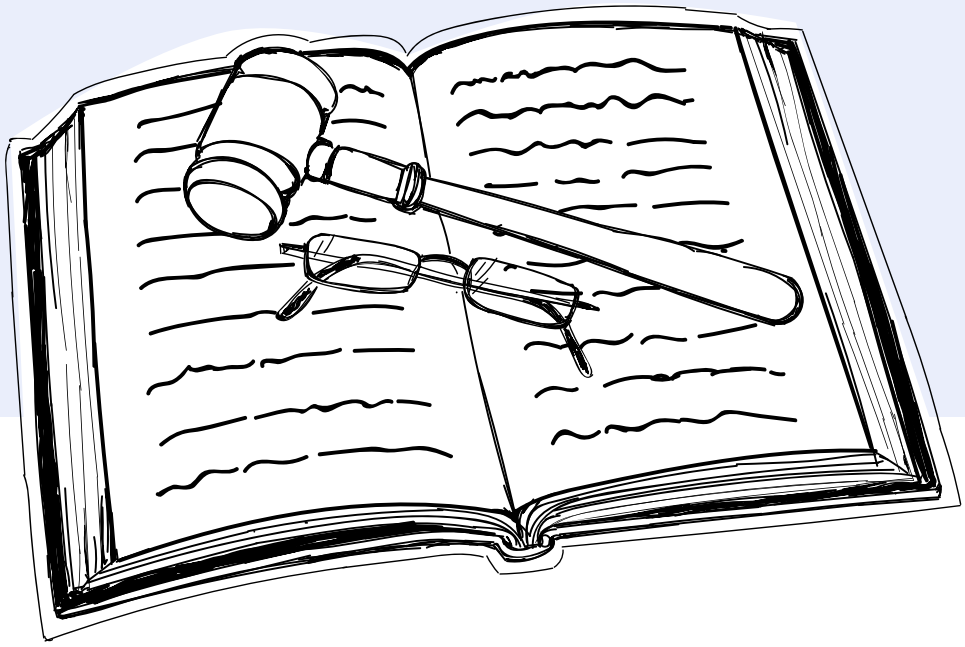
GDPR

and email outreach



Woodpecker

GDPR and Email Outreach

GDPR is one of the biggest updates to data protection since last 20 years and it's definitely worth to do some updates in your policy to become GDPR compliant. This PDF aims to make some clarifications for you and update you as far as GDPR compliance is concerned.

Author: Margaret Sikora

Cover: Justyna Bogusławska

Illustrations: Kinga Tarczyńska

Powered by Woodpecker.co

Table of contents

1 Territorial Scope

At first glance, the scope of GDPR application should be broader than that of the Directive 95/46/WE. What does it actually mean to us as EU citizens or people running business in the EU? Please have a look at the explanation below.

Where / to whom does GDPR apply?

- Data Controllers and processors present on the territory of the
- EU. If there are no facilities on the territory of the EU, but
  - Personal data belongs to EU citizens or people living on the territory of EU and processing is associated with offering them services or products.
  - Processing leads to monitoring the activity of EU citizens

REMEMBER!

GDPR assumes that Member States may enact some legislation around GDPR to bring it into action within their national legal system. It means that you may observe some differences from country to country in case of procedure.

A quick test - does GDPR apply to me?

My company is located within the territory of EU	Applicable
My company is located in the US (or any non-EU Country)	Not applicable
My company is located in the US (or any non-EU country) but I target European market and send my emails to Europe.Consequently, I use the EU citizen's data.	Applicable
My company is not registered in Europe, I don't target EU Citizens but my webpage is in Europe and I use EU member state's language.	Not Applicable

GDPR expands on the idea presented in the previous Directive, with the aim to grant an extensive protection to EU citizens.

Nevertheless, the relationship between an organizational unit and the EU needs to be evident. For example, if a company is not registered in one of the member states of the EU and it does not target EU citizens (individuals), there is no clear reason to apply GDPR in light of Art. 3 (2)(a) of the Regulation.

What about my national law?

GDPR is a regulation – that statement is repeated over and over again, but what does it mean?

As a regulation, GDPR is binding upon all Member States and it prevails over national law. EU law is characterized by a so-called 'supremacy doctrine' made up by the European Court of Justice.

The doctrine states that EU law comes first. A regulation, as a form of law,

does not require implementation, so it just enters national legal system without any introduction. Consequently, any national law undermining GDPR shall be said to be void and disapplied.

Where I can find this info?

Art. 3 of GDPR

Racital 22-25

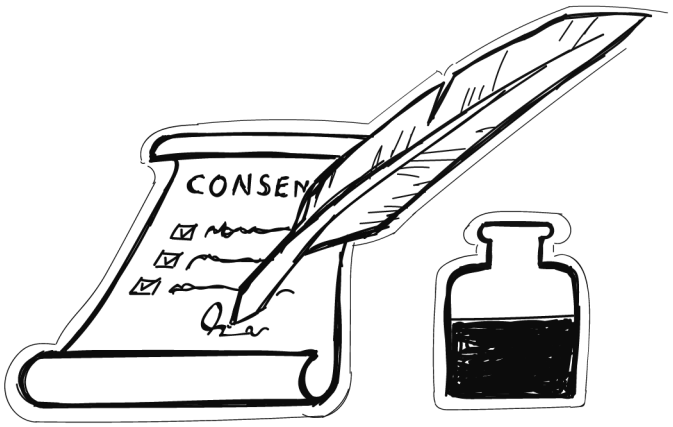
2 When GDPR enters into force, or becomes applicable?

GDPR has been operational since April 27, 2016. Nevertheless, the period of sanctions starts on May 25, 2018. Probably, we all know the famous statement that law does not work backwards. However, what if I have some prospects databases collected a year, a month or a week before GDPR enters into force?

To explain this one for you, here is a small case-based

I have some contacts collected before GDPR with consent forms. Is it necessary for me to do anything?	It depends, if your application forms contains some basic obligations derived from information duties then no. Nevertheless, if your consent forms miss some basics, like for example, storage limitation info or what data you process, then it will be definitely safer to resend a request for consent to your opt-in list.
I have some contacts collected before GDPR but I don't have a consent form. What should I do?	The question is, do you have any legal-ly justified ground to keep the data? If the answer is yes, then you can contact your prospects. But if you just have some old lists and you haven't used them or got any reply for months, the best solution would be to delete them.

I'm not sure how to collect consents in a GDPR compliant way, so I'll wait to see some practice afterwards.	This approach happens from time to time but it's very risky. GDPR lists some requirements as, for example, an easy way to opt-out, storage limitation, obligation to inform who you are, which should make you upgrade your consent forms as soon as possible. Of course, being data protection-friendly is not a one time action and you should upgrade your system continually, every time when some more precise guidelines are released.



3 Consent

In case you use email marketing in your business model, consent requirements are definitely something you should look into. GDPR is rather precise about what, where, and how you process personal data. Here you can find some more requirements to keep in mind once you make any consent form for your opt-in lists. There is no formal requirement concerning the consent form – there is no standard whether it has to be written or not, but definitely you should be able to prove that the person has actually given you a clear consent to process their data.

The consent has to be:

Unambiguous – nothing new here but there are some updates to keep an eye on due to GDPR. Once you set up a consent form, you need to remember that each person needs to know what he or she is subscribing to. Using pre-ticked boxes or assuming that silence implies consent is not good enough anymore.

Freely given – the consent is valid only if the person was able to make a choice. Any conditional deals, including limiting someone's access to the service due to lack of consent, shall not be accepted. Data subjects shall be able to express their consent to all processing elements separately to have a choice. It basically means that if you have under one tick consent forms to all marketing activities you should divide it into categories according to which you process personal data. For instance, you can divide it into a newsletter

communication, profiling, cold email campaigns, and so on, to allow data owners to choose what they agree to.

Specific – a consent shall be given to a particular thing. The moment of expressing a consent to everything at once and for all is gone. Now we need to collect consent in a much more accurate way. So if I run a newsletter for my product A and I have a list of subscribers who opted in to get the newsletter, I can't send them my newsletter about service B not mentioned in the consent form just because I also have this kind of service.

Informed – a person should be able to access all information concerning personal data processing. It is not only about the fact that you wrote it down somewhere and data subjects saw it, you should also show your due care to make the data subject understands the process.

Easy to withdraw – withdrawing the consent should be as easy as giving it. It is your obligation to ensure the person understands what to do to withdraw. Remember that opt-ins and opt-outs don't need to be the same in form. Their accessibility should be very similar though. If for an opt-in you use a link but you're unable to provide an infrastructure for an opt-out link, just place some information in your message stating something like: If you wish to withdraw your consent, please let me know via email at *name@woodpecker.co*.

EXCEPTIONS – in some cases, the consent needs to be explicit. Usually this is associated with special categories of data (sensitive) or special character of your activity. By explicit consent, I understand the consent which is given orally or written down (according to the interpretation of the Working Group of the Art. 29). For more information check Art. 9 and 49 of GDPR.

DO's and Don'ts

DO	DON'T
Precisely define your goal and aim in your consent form.	Don't hide what will happen with prospects data (no grayed out fonts)
Inform about how to unsubscribe/ request data deletion.	Don't pre-mark forms expressing consent – it should be a choice of your customer to mark it.

Clarify what is the subject of activity the person consents to. For example, subscription of your newsletter, receiving product updates.	Don't assume that silence or inactivity equals consent. You should always be ready to explain how the person consented.
Don't blur the real message. Once the person consent to an activity he/she should be fully aware of what is going to happen with his/her data.	Avoid group consent forms where you gather 3-4 different activities separate one from another because then how the person may consent to only one?
Give a way to stop data processing in a way which does not require any unnecessary effort and keep this info in each message.	

REMEMBER!

Consent is not the only legal ground which allows you to process data. It'll be discussed in the further parts.

Where I can find this info?

Art. 4 (11)
Art. 9 (2)(a)
Art 49 (1)(a)
Art. 7
Recital 32, 42, 43

4 Who am I? Data controller vs. processor

This question may be easily underestimated. Nevertheless, the question, “Who am I?” often helps us address more complex issues, for example, “What kind of obligations do I have?”

There are two possibilities in case of a who-am-I question. I can be either the controller or the processor. As usual, those definitions can be found in Art. 4.

Controller – the “main” person or subject responsible for data. By definition, the controller is a person or entity who defines the aim, extent, and all further details concerning processing. The controller is also responsible for the means of processing. As far as this pure division is concerned, if you run a marketing agency and proceed with some tasks or campaign that you were given by your client, you are the processor, and your customer is the administrator of data.

Processor – chosen by a controller, processor takes any action on data due to the will and on behalf of the controller, profiling, cold email campaigns, and so on, to allow data owners to choose what they agree to.

Some people wonder what information duty does cover, and what sort of info should be passed along to the data owner. Remember that if you use any processors or sub-processors, you, as a controller, should inform the data

subject about the processing. Also, you are the one who's responsible, so try to choose smartly. If you are simply unable to verify on your own whether your processor is GDPR compliant or not, just ask them.

Where should I look for to check if my processor or sub-processor is GDPR compliant?

- Terms of Service (example: https://woodpecker.co/terms-of-service/)
- GDPR Compliance published on the website (example: https://woodpecker.co/gdpr-compliance/)
- Data Protection Commitment – a unilateral document may be additional to Terms of Service with extra commitments binding upon the processor.
- An existing possibility to sign Data Protection Agreement or Addendum to the Agreement.

Side note! If you wonder what sort of documents you should give your customers this list above works for you as well. By compiling documents like those, your customers can check your GDPR compliance and potentially get documents which are necessary for them to be legally safe and transparent to their customers.

Where I can find this info?

Art. 4 (7) and Art. 4 (8)

5 GDPR and email marketing (subscription lists)

A fuss about GDPR and sending cold emails started with a consent-based approach. There were a lot of myths, concerning sending in accordance with GDPR. In the discussion about news and updates, we shouldn't lose sight of the core element. Namely, GDPR is not about marketing your product/service, it is about protecting personal data.

If you manage subscription lists, you should definitely pay attention to GDPR. First of all, GDPR places much importance to the consent rules described beforehand. If you use subscription lists, there are key elements which you should double check to make your GDPR compliance form is ready to go.

- Consent must be actively expressed, it cannot be implied, i.e. given through silence or inactivity.
- The access to a service mustn't be made conditional on the consent to other activities, which are not necessary to perform the service.
- How do you store your consent forms? Remember that you need to be able to show and prove the consent.
- Data subjects are allowed to withdraw consent at any point.
- Create separate consent forms for different aims of dara processing.
- How do you obtained my opt-ins before GDPR entered into force?
- Is there any information about storage limitation in your consent form?

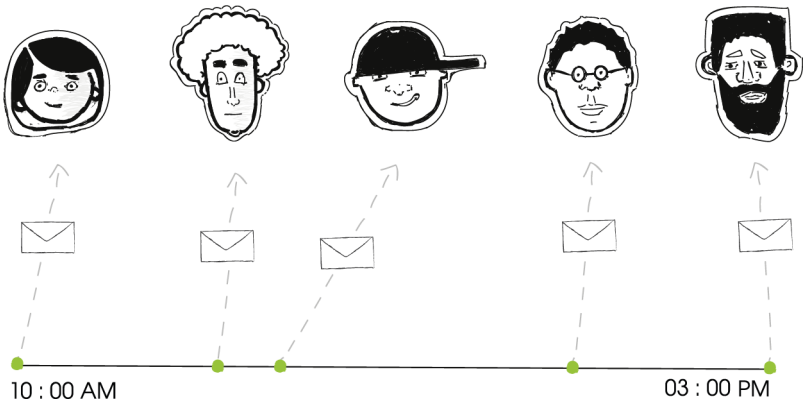
To make this complex situation more readable check our situation-based compliance explanation.

SITUATION	GDPR COMPLIANT RESPONSE
I have a list of subscribers and I've collected the consent before GDPR became so well-known. I had some of GDPR-required elements in there but not all of them.	In this situation the best option would be to re-send your opt-in list. Of course, there is always a risk that some subscribers will not opt-in again but this would be definitely the best process to go through. You may always send more than one reminder about opt-in to let your subscriber choose what is desired by them.
I run a service and once someone becomes my trial or premium user, the person is automatically requested to agree to process their data due to marketing purposes.	This is not GDPR compliant. Once you have consent form and once you wish to use the service you're "forcing" to accept marketing communicatio you're actually overcrossing what is accepted by GDPR
I sign agreements with my customers so I assume their consent is implied to send them any emails I have planned to send.	Remember that having an agreement with your users or customers does not entitle you to process their data without any limits. Even if there is a contractual relation between you and your customer you should still be able to show that the person consented to any activity not related to the pure performance of the contract. It means that you cannot require from your customers to agree for all marketing correspondence just because they purchased your product.

To sum up, before you start sending make sure that all what you have in your email is GDPR compliant. Simply think if this is clear for your prospects to unsubscribe as easy as opt in. Think through your current opt-in list and try to evaluate if consent was collected in GDPR compliant way? If you have any doubts go to Consent checklist above.

Where I can find this info?

Art.4, Art.6, Art.7, Art.8, Art.9 Recital 32, 33, 42 and 43



6 GDPR and cold emails

Opt-in forms for sending newsletters and messages seems to be quite obvious for people who are already familiar with GDPR. Nevertheless, there's always a tough question, *"Should I send my cold email campaigns only to opt-in lists?"*

Cold emails have a very unique nature, and as we all know, there is no paragraph nor recital in GDPR which says that you can send emails to contacts on opt-in lists.

To explain cold emailing under GDPR, let's focus on the following elements:

- Who am I?
- What is my legal basis for processing?
- What tools do I use?
- How I store the data, and for how long?

Those 4 questions will help you to

a) diagnose your situation

b) plan what you can and cannot do

So, who am I?

Be aware of your role. In terms of GDPR, you may be a controller, processor or sub-processor. Let's look at some case scenarios. But first, a quick reminder what are those roles.

Controller – decides about the aim and purpose of processing, that person is the "reason why" processing happens.

Processor – processes data because the controller asked him/her to do so and makes it on his/her behalf.

Sub-processor – employed by the processor to help in data activities.

I have an outbound team at my company. I collect data and send cold email campaigns to generate new customers.	Controller
I run a lead generation agency and I help customers to generate leads.	Processor
I run a company but I don't have my own outbound team – I use a lead generation agency.	Controller
I provide a service which automates sending process for my customers.	Processor
I run a company that delivers a product used by third parties to make an automation tool to send emails.	Sub-processor

As soon as you know who you are, you can answer some simple questions which concern not only sending process but also your internal company organization, let's look at the examples.

- Do I have to do Risk Assessment?
- Is it necessary for me to have Data Protection Officer?
- Should I sign a Data Protection Addendum with anyone?

All of the above questions should be consulted with a lawyer. Either way, an initial in-company research will definitely help you to go through the process smoothly.

Now coming back to cold emails, you should know by now what's your role. By this you can easily fulfill the first information duty – tell your prospect who you are.

What is my legal basis for processing?

This question was asked countless times – when it comes to cold email outreach, a legitimate interest which "justifies" data processing is included in Art. 6 (1)(f) and recital 47. To get a full grasp on what it means, let's have a look at the excerpts.

Art.6 (1)(f)

Processing shall be lawful if […]
processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Recital 47

The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal

basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.

The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Yes, that's a long explanation, but it confirms that using data for direct marketing may be considered as a legitimate ground for processing. Since cold email outreach fits perfectly into that category, we have our legal basis for processing interpreted!

What tools do I use?

If you employ any third party tools which transfer data outside of the EU, you should be careful because you may be obliged to inform your prospects about this! Because of that, before you start your GDPR-compliant campaigns just prepare a list of your processors/sub-processors and evaluate them with GDPR in mind. Maybe you'll find some GDPR compliance forms on the processors/sub-processors websites, or a possibility to sign a Data Protection Agreement.

If your tools come from the USA, don't panic – there is a well-known Privacy Shield agreement made between the European Commission and the USA which establishes that the USA is a safe country for data transfer. Despite all of that, you can still check if the tool you use is Privacy Shield certified. That will definitely benefit your data safety.

Some of you may wonder why you need to ask yourself that question before doing cold email campaigns? Usually, sending cold email campaigns implies data processing on a large scale, and consequently, we may need to assess the risk of data leak for ourselves and our customers.

How do I store the data, and for how long?

This is the last question to ask yourself when doing email outreach, and one of the final obligation duties. Inform your prospects that you'll keep their data for, for example, 30 days since they open the message and after that time, the data will be deleted from our contact base. Also, let your prospects know how to request data deletion.

Now frequently asked question – why is it 30 days? In GDPR there is no settled day limit for data processing to be proportionate and adequate. There are, at least now, no guidelines concerning how to establish that.

There's one thing we know, namely, it is better to have a limit than not to have any limit. Of course, once GDPR enters into force, there may be a need to reassess that part. But until that happens, we at Woodpecker, internally agreed that 30 days is a reasonable time limit – but remember it's up to you.

Due to an explicit requirement in GDPR not to process data for longer than necessary just set a limit for yourself. Just choose the one you can justify. An important caveat – don't assume that what is necessary is forever because that's a huge stretch.

- Tell your prospects who you are
- Inform them about the aim of processing
- Inform them about processing time limit
- Let your prospects know how to opt out
- Let your prospects know how to request data deletion/correction/return

Where I can find this info?

Art. 6 (1)(f) of GDPR

Racital 47

Art. 5

Art. 4

Woodpecker