sendwithus
Dyspatch

Marketing for Consent

How to Make GDPR Compliance Work for You

The following is intended for informational purposes only and should not be construed as legal advice.

Almost every marketer will recognize the truth in the following two statements:

1. Customers want exceptional, personalized, relevant brand experiences, and if you don't provide them, they'll find a competitor who will.

2. Customers are reticent — and rightfully so (think the 2017 Equifax security breach) — about sharing the personal data brands often need in order to deliver those experiences.

The tension between these two facts can leave your business between a rock and a hard place. And to compound this difficult position, marketers are facing ever-more stringent data privacy regulations that further impede their ability to collect, store, and use customer data.

Welcome to the age of GDPR, the European Union's General Data Protection Regulation.

> **If approached in the right spirit, GDPR compliance can be a win-win for email marketers, quite possibly providing a much-needed correction.**
>
> **Matt Harris, Sendwithus co-founder and CEO**

When viewed through the lens of optimizing the Customer Experience, the GDPR can actually be seen as good news. (No, we're not kidding.)

How often have you, as a marketer, formulated an exciting new way to improve CX only to run into a wall constructed with some combination of the following bricks:

- "There's no room in the budget."
- "We don't have anyone with the right skillset to pull that off."
- "We don't have the right tools in place."
- "Our data and processes are too siloed for that kind of holistic approach to be feasible."
- "The CMO says it's too risky."
- [insert your excuse of choice here]

But if GDPR compliance is required for your business, you have no choice but to find the money, the people, the tools, the executive support, etc., to meet the requirements. While the intention of the GDPR is data protection for individuals within the EU, a happy side effect of compliance will be the smashing of more than a few of those obstacles.

GDPR Penalties:
Fines for violating the provisions of the GDPR can be up to €20 million, or 4% of annual global revenue, whichever is higher.

So stop thinking of compliance as an unpleasant necessity to avoid penalties and instead approach it as a massive opportunity to improve customer relationships. In so doing, you'll soften both the rock and the hard place mentioned earlier, allowing you to implement processes that will earn your customers' trust and encourage them to willingly share the data you need to create the exceptional experiences they expect.

Think of it this way: What's good for GDPR is good for your customers and what's good for your customers is good for you.

Successful marketing under GDPR boils down to four basic principles:

1. Embrace the fact that the customer owns their data. Allow your customers to choose when, where, how, why, for how long, and what they choose to share with you.

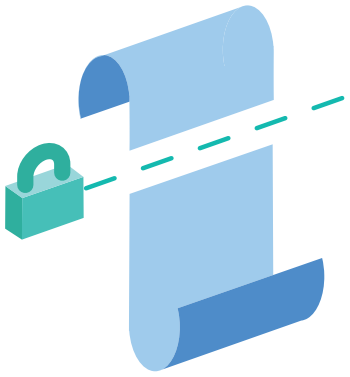
2. Give the customer an excellent 'what's in it for me' reason to share their data. Present a compelling case for the exceptional experience their data will allow you to offer. And deliver.

3. Invest in precision insights over bulk data. Precise information about a smaller number of deeply invested customers will allow you to provide the kind of personalized experience that will both keep those customers and attract more like them.

4. Get your data collection and consent processes right and make sure they're scalable.

The Data You Already Have

This might be a good time to mention that there is no grandfather clause under GDPR. Its provisions apply to personal data you collect and use going forward, as well as to all the data you ***currently*** have. If you haven't already, you should do a complete audit of your current data.



You don't have to go as far as JD Wetherspoon, a UK chain of pubs, who decided the risks were too great and deleted their entire email list last year. (A bit of a short-sighted, over-reaction, if you ask us.) But you do need to purge everything that is old and/or that belongs to customers who no longer demonstrate engagement with your product, service, or content.

For those customers whose data you do wish to keep, you might be fine if you can demonstrate an existing relationship but general consensus is that may be difficult to prove. A much better plan is to reach out and request new consent, even if they opted in at some point in the past. Your request must be specific about each piece of data you have and each purpose for which you will use it. You must also provide information on how the customer can access their data and have it corrected, deleted, or moved to another provider.

Even if You're Not Located in the EU

Whether or not the GDPR is applicable is about the *customer's* location, not yours. And it's about the customer's *location*, not their citizenship.

This means that while the GDPR does apply to the processing — (read on for the GDPR's definition of 'processing') — of the personal data of EU residents by companies located in the EU, it also applies to any company, anywhere, that processes the data of any individual located in the EU, regardless of that individual's citizenship. This means, for example, that a US citizen living in Paris will enjoy the protection of the GDPR but a French citizen living in Chicago will not.

So if you do business with residents of the European Union and you want to continue to do so — which is more than just good business sense, since excluding the population of an entire continent from your existing and potential customer base would probably require as much technical effort as compliance — then the GDPR applies to you.

And while it might be tempting to establish one GDPR compliant set of processes for EU residents and another for those outside the EU, don't. Just don't. Your non-EU customers, including that French citizen in Chicago, won't thank you. Better to establish GDPR compliance, with the improved transparency, security, and trust that go along with it, for all your customers, no matter where they live.

May We Borrow Your Data, Please?

Marketers have spent the better part of the last two years collectively wringing their hands over the GDPR's consent requirements. *What? You mean I have to ask for permission to market to people?*

Yeah, you do. But even without the GDPR, you should probably be doing that anyway.

28% of marketers say consent is their primary concern about GDPR.

Source: emarketer.com

Before you get too worked up, consent is only one of six legal grounds for data processing under the GDPR. Those legal grounds are when data processing is:

- Necessary for the performance of a contract
- Necessary for compliance with a legal obligation
- Necessary to protect the vital interests of a data subject
- Carried out in the public interest or the exercise of official authority
- Necessary for the purposes of the legitimate interest of the controller or a third party
- Or when the data subject has given consent

The last two, legitimate interest and consent, are the two that will apply most to marketing activities. Let's take a look at what GDPR actually says about them.

Article 4(11): " 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Article 6(1)(f): "Processing of personal data is legal if it is necessary for the purposes of the legitimate interests pursued by the controller or a third party."

Recital 47: "The legitimate interests of a controller…may provide a legal basis for processing… The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

Even though 'direct marketing' is specifically named as falling under legitimate interest, the language that surrounds it is pretty vague and open to interpretation. So rather than pulling your hair out trying to figure out how you might prove a case for legitimate interest if asked, it probably makes more sense to just ask for consent. Your customers will appreciate your transparency and if their consent is freely given, specific, informed, and unambiguous, and you document it adequately, you'll be able to easily demonstrate that to authorities.

So how do you make sure your consent requirements comply with those of the GDPR? Here are some basic guidelines.

Data Subject Rights:
The GDPR defines data subject as 'a natural person whose personal data is processed by a controller or processor'. The GDPR establishes the following data subject rights:

Right of access: You must provide full access to personal data upon request by a user.

Right of information: You must clearly inform the user how their personal data is collected and how it will be used.

Continued on the next page…

Clear and concise consent requests:

When you ask for consent, make it clear what you're asking for, why you're asking for it, and what you'll do with it. Use plain language that's easy to understand. Ultimately, it must be simple for the customer to understand what they need to do to grant consent, what will happen when they do, and how they can change, rescind, or transfer their consent at any time.

Make your requests concise but with more detailed information available either through links, hover-over pop-ups, or by a similar method. If 'what you'll do with it' includes sharing with a third party, make it clear who, why, and what that third party will do with the data you'll share. (You also need to make sure the third party is GDPR compliant as well, but more on that later.)

You must also provide explicit information on how the customer can cancel or change their consent, as well as how they can change, delete, or transfer their data to another company.

A separate request for each processing activity:

Processing is defined under GDPR as pretty much anything you can do to or with data, from collection to storage to analysis to deletion, and everything in between.

If you want the official definition:

Art.2(b): ""Processing" means any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

Right to rectify & to be forgotten: You must provide a method for a user to have their personal data modified and/or deleted upon request.

Right of portability: You must provide the user the ability to retrieve their data in a readable and usable format so that they can move it into their own possession or to another controller.

But that does not mean you should ask for consent for everything all at once. That would be very bad. Remember, the title of this section is, 'A separate request for each processing activity'. You can no longer simply bury multiple consent requests within a massive 'Terms of Service' document and call it done.

Especially since 'Purpose Limitation' and 'Data Minimization' are also part of GDPR.

- **Purpose Limitation** - Personal data should be collected for a specific, explicitly stated purpose and not used for anything else
- **Data Minimization** - The processed data should be limited to what is necessary to achieve the stated purpose

Take a breath. It's not as complicated as it sounds. All this means is that you should only request consent for the minimum amount of data you need, for the specific purpose for which you need it, at that particular point in the customer journey.

A request for consent to track browsing behaviour by cookie or tracking pixel when they land on your site. Another for an email address when they request a downloadable piece of content. One asking for frequency preferences when they opt-in to marketing emails. Ask only for what you need, only when you need it.

Bear in mind that these requests will very rarely happen within the same session, the same day, or even the same week or month. So the chance of annoying your customers with a barrage of consent requests is minimal.

And that just makes sense. If you keep your consent requests small and precise, staggered throughout the customer journey, you'll not only minimize possible resistance, you'll establish a level of transparency that will incrementally build trust along the way.

An affirmative and unambiguous expression of consent that is freely given:

Again, this isn't as complicated as it sounds. 'Affirmative' means consent must be given by a positive action, such as saying 'Yes', checking a 'Sign Me Up' tick-box, or clicking the link in a double opt-in confirmation email. Passive opt-ins, such as a tick-box that is pre-checked by default or a failure to opt-out, are not considered affirmative consent under the GDPR.

The 'unambiguous' part simply means that a customer's consent must be clear, precise, and not open to interpretation. (Unlike that legitimate interest language… but we digress.)

Finally, the 'freely given' part means the customer's consent must have no bearing on your ability or willingness to deliver goods or services to that customer. In other words, you can't deny service based on a customer's refusal to grant consent. Nor should you make special offers, rewards, prizes, etc., contingent upon the granting of consent.

Just to be clear, this does not apply to data that is necessary for the delivery of a product or service. You can still collect the data you need to process an order or the data necessary to deliver a downloadable piece of content, for example. You just can't make delivery contingent upon receiving consent to use that data for other purposes, such as opting in to receive marketing emails. Both situations are prime opportunities for requesting consent but you can't refuse to deliver if consent is not granted.

Asking for Consent Won't Kill Your Email Marketing

Unless you choose to let it. The truth is that adding customers to marketing lists *en masse* was never a great idea in the first place. Marketing to people who don't want it has always been a sure way to lose customers. But because we spent so much time focusing on list size rather than list quality, it took us longer than it should have to figure that out.

By shifting your focus to list quality, you can achieve GDPR compliance while improving the customer experience. And you may actually increase your email ROI along the way. Here are a few tips to help you get there.

Establish Double Opt-in

When asking customers for consent to send them marketing emails, make sure you use a double opt-in process. And do it well.

A double opt-in adds a second step to the subscription process. The customer submits their email address and you follow up with a reply email that includes a link for the customer to confirm their subscription. Clicking that link is how the customer grants consent by an affirmative action.

What the customer sees when they click the link can be as simple as a message saying, "You have successfully subscribed," with the required messaging around how the customer can cancel or change their consent, how they can change, delete, or transfer their data, and the mandatory link to your Privacy Policy. But you can do better than that. Remember what we said about doing it well?

Your 'subscription successful' page should also inform the customer what to expect in terms of email types — content digests, new product announcements, special offers, discount coupons, etc. — and frequency — daily, weekly, monthly, etc.

If you want to do double opt-in extremely well, you can provide a 'Preference Center' and

give the customer the opportunity to choose their preferred email types and frequency. Retailers can also let the customer choose the product categories they're most interested in hearing about, while content providers can offer topic selection.

You might also want to consider providing the customer an opportunity to provide additional — and fully optional — data points that will allow you to customize their experience even further. Make it absolutely clear how the data will be used and ask for consent by affirmative action.

If you're concerned about overwhelming your customers with too much, too soon, Preference Center options and additional data requests can also be rolled out gradually, over time, through website content, ads, blog posts, or an engagement-based drip campaign. If you choose to go with a Preference Center, make it the destination for the Unsubscribe link in your emails and provide easy-to-find access to it on your website.

By establishing a double opt-in you'll not only be in compliance with GDPR, you'll also create a database of customers who are truly interested in what you have to offer. Your list might shrink a little — or a lot — but engagement will improve immensely.

Optimize Transactional Email

So where do transactional emails fit into all of this?

Transactional emails are sent to an individual as a result of an action triggered by the user or that are necessary as part of an ongoing, existing relationship with the user. They include order confirmations, password resets, shipping notifications, receipts, legal notices, policy updates, etc.

As such, consent, as it's defined for marketing emails, is not required for transactional emails.

However, transactional emails do use personal data. So it is imperative that during the collection of that data — during account creation, checkout, password reset request, etc. — you include information on data privacy and security, including assurance that the data will be used solely for the intended purpose.

Your transactional emails themselves provide a prime opportunity to reinforce transparency and trust messaging, as well as to (subtly and tactfully) solicit opt-ins to email marketing. Conduct frequent tests in order to refine your message and achieve the best results.

I know what at least some of you are thinking. Test transactional emails? But how? If your transactional emails are owned by product teams or IT, you probably need to rely on developer resources to update their content. And with this whole GDPR compliance process, you've likely already exhausted any developer goodwill you may have had stockpiled. So what's the solution?

The best option is to find a way to get transactional email out of the code base and into some kind of email template management system that allows you to edit the content without relying on developers. Additionally, separating email content management from customer data will go a long way toward achieving compliance.

They may be hard to find but such systems do exist. (Just ask us. We know a good one.) The right system will allow you to easily create, update, test, and optimize your transactional email content, as well as seamlessly manage localizations for your global audience. Want to add product recommendations to order confirmations for your US customers but not for those in the EU? No problem.

Separating email content management from your code base and your customer data will not only help with compliance, it will also help you achieve consistency in branding and reputation management, significantly improving the customer experience.

A Word About Third Party Solutions

While we're talking about a third party email template solution, it's worth noting that every system that touches email, both transactional and marketing, must be GDPR compliant. As a 'controller', you're probably already on top of compliance for your in-house systems — and if you aren't, you should be — but you should also be cognizant of any third party solutions you use.

And this doesn't just apply to systems that touch email. You should be reviewing your agreements with all third party providers that touch your customer data ('processors') and updating them to include GDPR compliance. Everything from your CRM, your marketing automation platform, cloud-based data storage services, your email service provider, analytics and segmentation software, and even your email template editor — they all must be GDPR compliant. Vendors should be able to demonstrate their compliance and you should get it in writing, in the form of updated vendor agreements that include an action plan for any potential breach or enforcement action.

If any vendor is unable or unwilling to meet GDPR compliance requirements, you should be looking for one who is.

Controller vs. Processor:

Controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Automated Drip Campaigns

The GDPR also includes provisions regarding the use of data in customer 'profiling', which is defined as any automated processing of personal data to evaluate, analyze, or predict any characteristics or behaviour of a user. The GDPR provides specific protection against automated decisions based on profiling.

These provisions are intended primarily to guard against automated decision making around things like granting or denying credit or employment based on profiling. But they also apply in the case of automated drip campaigns, such as onboarding campaigns for new customers

or new blog subscribers, or nurture campaigns based on content downloads (ebooks, white papers, etc.), where decisions about future emails in the campaign are automated based on user behaviour (clicks, opens, reads, etc.).

The good news is that automated campaigns can still be compliant if the following conditions are met:

- You notify the customer up-front how you intend to use their data
- You request and are granted consent to use their data for the stated purpose
- You provide the opportunity to opt-out of all such profiling, both up-front and at any time thereafter

Drip campaigns are the perfect opportunity to *'market for consent'*.

Marketing For Consent

Marketing for consent simply means using your considerable marketing skills to make a compelling case for the exceptional customer experience your campaigns will provide, encouraging your customers to provide both the data you need and the consent to use it.

Earning consent should be as important as earning conversions.

You're already mapping out the customer journey and crafting your message for every touch-point along the way, so why not include built-in messaging and processes to optimize the receipt of personal data consent? If you clearly demonstrate 'what's in it for me' for your users, they'll be more likely to grant their consent. Just be sure to build strong trust language into your messaging and then earn that trust by delivering on what you promise.

In the case of customers who've made a purchase or downloaded a piece of content, they're customers who have already demonstrated engagement with what you have to offer. Once you've delivered quality in the form of your product, service, or content, and demonstrated that you're worthy of their trust, a consent request will not be out of place. You may find customers will be more than just willing to grant consent, they'll be eager to do so.

Don't forget that this isn't a pass or fail test. Even if the customer doesn't grant consent the first time you ask, you can continue making your case through website copy, ads, blog posts, etc., and then ask again. And just as with all your other marketing initiatives, test and retest your consent messaging to continually optimize and identify which message, at which points in the customer journey, will provide the best results.

sendwithus

Dyspatch

Dyspatch is a cloud-based communications management platform that helps Enterprise organizations centralize their email creation, approval, and publishing processes. The powerful API, visual editor, and built-in device testing allow for cutting-edge email strategy and execution, while helping establish consistency in both branding and legal compliance across multiple teams.

sales@dyspatch.io

dyspatch.io

3252 19th St, Unit A, San Francisco, CA 94110