

GDPR Readiness Guide

What is GDPR?

You may have been hearing a lot about General Data Protection Regulations (GDPR) lately. And with good reason. It's a big undertaking that has a significant impact on businesses all over the world. We've been hard at work ensuring you're protected as our customers, and are taking additional steps to ensure you're prepared to serve your own customers in this new GDPR reality we'll all soon be living in. In fact, if you have a single customer (or prospect) based in the European Union (EU), this may impact you. Don't panic. We're going to help you get prepped.

Here's the gist: from a very high level, this is the EU's initiative to update outdated laws that protect users and their data. In essence, it gives EU residents more authority over who is using their data and how. And rest assured that as GDPR laws evolve and become even more defined, we'll stay informed and current in our own practices as well as the features we extend to you.

The more detailed description of GDPR can be [found here](#).

How to use this guide

We're just going to come right out and say it. GDPR is complex stuff. But we've been preparing in an effort to make it an easier process for you, adding features and campaigns to help you automate your GDPR compliance as much as possible.

This guide isn't meant to explain the entirety of the GDPR articles. It's meant to make it easier to be GDPR-compliant within the scope of the Infusionsoft product.

Now for the disclaimer, and it's a big one...

DISCLAIMER: We can't interpret the law for you. We're not sanctioned legal representatives. However, we've done our best to make a complex topic more understandable and actionable for you. Please consult your legal advisor.

That said, let's dig in and get to know GDPR.

Data roles

We could probably spend a long time waxing poetic about this. But what fun is that? Instead, let's just make these roles and responsibilities clear.

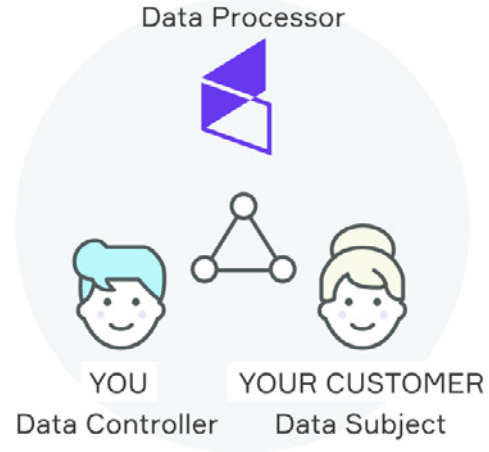
There are three roles in any data-related relationship:

- Data Processor
- Data Controller
- Data Subject

Here's a hypothetical scenario to help define each...

You are a customer of Infusionsoft and utilize us as your **data processor**. We are responsible for processing and safeguarding your customers' data.

Because you actively use our platform and enter client data, that makes you the **data controller**. Let's imagine you have a customer in Italy named Liliana. She's your **data subject**, and she relies on you to honor her requests regarding what, how, and when you process her data.



Remember Liliana because she's going to come back into play when we start defining the different articles of the GDPR.

GDPR Checklist

We've provided functionality to help you ensure the Infusionsoft portion of your business is GDPR compliant. The functionality will be ready on 22 May 2018. You'll see action items that indicate steps to take inside of your account in the column titled, "Your Infusionsoft Checklist" after the 22nd.

There are other steps you'll want to take outside of your Infusionsoft account to prepare yourself for GDPR compliance. Look at the column titled, "Additional Actions" for those recommendations.

Speaking of recommendations, this is where we remind you once again about the giant disclaimer we called out at the beginning of this guide. We can't interpret the law for you. These are simply suggestions for what you can do within your account to prep for GDPR as well as some additional (non-sanctioned) recommendations.

GDPR Requirement & Explanation

Your Infusionsoft Checklist

Additional Actions

Right to be Informed

You need to tell your customers how you plan to process their data, how you won't process their data, and when you'll be done with it.

Add a link to your privacy policy on all web forms, landing pages, order forms and shopping cart (i.e. wherever you collect personal data). [How to link to your privacy policy.](#)

If you choose to obtain a customer data in other areas of your business (e.g., in person), you'll need to make sure your privacy policy is accessible within that interaction.

Lawfulness of Processing

In order to process someone's data (e.g. market to them), you need to have a legal basis for doing so. That could include these valid scenarios:

- Informed Consent. This means the contact gives you specific and explicit consent to process their data (e.g. agrees to receive email communication from you) [[See Consent Section Below](#)]

Create set of new tags to track the lawful basis for each contact. You'll need to provide this in case of an audit: [How to create Lawful Basis tags](#)

Apply the appropriate tags to your current contacts to ensure that you are tracking the lawful basis for each contact: [How to apply tags to individual contacts](#)

Consider how you'll track lawful basis for contacts you acquire outside of Infusionsoft according to Lawful Basis of Processing to ensure you're compliant online and offline, and in case you're audited in the future.

- Performance of Contract. You need to process a contact's data in order to perform a contract. This may include delivering a product or service along with relevant communication. When fulfilling goods or services, you can only fulfill what was agreed upon without delving into pushing additional services. I.e., don't spam customers in the midst of a business interaction.
- Legitimate Interests. You have a right to market your products and services to fulfill your legitimate business interests, as long as you're properly balancing your interests with the data privacy and protection rights of your customers. Evaluating this balance can be tricky, especially when the nature of the data you are collecting is highly sensitive. Your DPO and legal advisor can help. This one is complex. For a more in-depth exploration, take a [look at this](#).

- Configure your existing webforms, landing pages and product purchases to apply lawful basis tags automatically:
[How to configure webforms & landing pages](#)
[How to configure product purchases](#)
- Create a regular process to remove EU contacts where you no longer have a lawful basis to process their data:
[How to remove your EU contacts](#)

Consent

There are a few requirements to consider in order to use Consent as your lawful basis to process data for a contact:

- You must be clear about what consent you're asking for (more specificity is better, including a reference to your privacy policy).
- Don't pre-check your consent checkboxes. This ensures that your contacts are explicitly giving consent.
- You need to be able to show proof of consent for prospects and customers who have granted it.

Hypothetical example:

Liliana registers for a free webinar and is given a clear option to consent to receive updates, news, and other marketing from you via email, in accordance with your privacy policy.

Obtain consent from existing EU contacts for whom you don't have consent (or any other lawful basis to process):

[How to use the GDPR Helper Campaign](#)

Update all web forms and landing pages with GDPR-compliant consent checkboxes:

[How to add consent checkboxes](#)

Implement these guidelines anywhere else in your business where you ask for consent or personal information. (e.g. an in-store Point of Sale register or a paper signup form at an event).

Consider creating **documentation** (with a timestamp) any time you make changes to your consent checkboxes or privacy policy (include screenshots). This is important so that you can show the exact text your contacts agreed to. This information is not captured inside Infusionsoft automatically.

Right to Object, Right to Erasure, Right to Restrict Processing

If a person wants you to stop processing their data, they can request to be erased from your data records completely. It should be as easy to withdraw consent as it was to give it.

In some situations you may feel you have reason to deny this request (e.g. you have a contract to fulfill). If this happens, you'll need to pause your marketing until you come to a resolution and get consent from your customer.

Hypothetical example:

Liliana signed up for your newsletter last year when she was very interested in your area of expertise. Things have changed though and she'd like to not only unsubscribe, but stop engaging with your business entirely. She needs an easy way to request that you remove her from your database.

While a customer can make this request, it's up to you to carry it out.

Create a simple way for your customers to request to be erased:
How to use the GDPR Helper Campaign

Use the new "Anonymize Contact" feature to safely anonymize contacts who request to be forgotten. *This can be performed at your discretion, especially if this customer has outstanding business obligations, like an unpaid invoice.

New feature How to anonymize a contact

By sending emails using Infusionsoft (broadcasts or campaigns) your contacts will be able to request to have their data erased as part of the opt-out process. This will automatically notify you that a request needs your attention.

New feature How a Contact Exercises Their Right to Erasure

We've released a feature that will allow you to prevent yourself from inadvertently adding a contact to Infusionsoft when they'd previously been erased.

New feature How Anonymous Records Work

You'll be responsible for carrying out your customer's request to erase their data and can do so within your account. Make sure you have an internal process to monitor requests and ensure they are handled in a timely manner.

If you keep customer contact records or data outside of Infusionsoft, you'll need to erase those as well.

The Right to **Data Access** and **Portability**

Your customer has the right to know whether their data is being processed. If you are processing their data, they have a right to know what you're processing and should be able to request access to see it in a portable, visually-friendly fashion.

Hypothetical example:

Liliana has been a customer of yours for a long time, but has recently become more concerned with data privacy. She'd like to see what you see as it relates to her data profile. She may want to do this for a variety of reasons, from general curiosity to needing to process a name change.

- Create a simple way for your customers to request access to the data you are processing for them:
[How to use the GDPR Helper Campaign](#)

There are a few ways you can fulfill this request within Infusionsoft:

- You can [take a screenshot](#) of the customer record and send it
- You can export a contact's details in a CSV file and send it
[How to export contacts to a CSV file](#)

- You'll be responsible for carrying out your customer's requests quickly. Make sure you have an internal process to monitor requests and ensure they are handled in a timely manner.
- This right to access and portability is not limited to the data in your Infusionsoft account. You'll need to find a way to collect other pertinent data for your customers and transfer it to them securely.

Right of Rectification

Your customer has a right to see their data and ensure its accuracy. If errors exist, they have the right to request you update that information (and any other instance of that data that you control) in a reasonably expedient manner.

Hypothetical example:

In the previous example, Liliana requested her data and saw an error. Her email address was listed as @yahoo rather than @gmail. She can request that you update her email address in all of your systems. In addition she may request that you pause all marketing efforts until you make this correction.

Alternately, Liliana could have gotten married and be actively reaching out to companies she does business with frequently. She may not necessarily need to see a mistake before requesting you make an update.

Create a simple way for your customers to request that you update their data:

[How to use the GDPR Helper Campaign](#)

Update the Infusionsoft Contact record with the requested changes.

Make sure you have an internal process to monitor data update requests and ensure they are handled in a timely manner.

In addition to updating Contact in Infusionsoft, you'll also need to update the customer's information in other systems and notify any other authorized 3rd parties that process your customer's data.

Designation of data protection officer

You'll want to appoint a Data Protection Officer (DPO). What does that mean exactly? Simply that you should acquire your own professional guidance to ensure you're GDPR compliant. While using Infusionsoft can help, we can't assume the role of compliance on your behalf. Here are some [good guidelines](#) for identifying a DPO.

In addition, you'll need to appoint a **Chief Data Security Officer (CDSO)**. This person will have the authority to handle any complaint regarding security and privacy. This will most likely be you if you have a small company or are a solopreneur, but you may also decide to appoint an IT or legal representative employed by your company.

In addition, you'll need an **EU representative** to handle any data or security dealings in the EU specifically. This person must be an EU citizen or resident. Now, if you don't have a person that fits this description, you may also opt to have a third-party company or representative based in the EU fill this role. For example, Infusionsoft chose Verasafe Ireland to fulfill this role for us.

In addition to identifying the right people to fill the three roles mentioned, you'll need to:

Sign the Data Protection Agreement. You can find this in [Settings](#) in your account.

New feature

Enter your Chief Data Security Officer and your EU Representative in the [Privacy & compliance settings](#).

New feature

Appoint a DPO, CDSO and EU Representative.

Add the individuals who fill these roles to your privacy policy.

More resources

Hopefully the step-by-step instructions for each of the checklist items will help you take care of preparations for GDPR within your Infusionsoft account. We know this is a complex topic and you're likely to have many questions. Please feel free to browse these resources to dig a bit deeper.

- [Frequently Asked Questions and Answers regarding GDPR](#)
- [General Data Protection Regulations \(GDPR\) full text](#)
- [The EU Will Start Enforcing the GDPR Soon—Is Your Business Ready?](#)
- [GDPR Help Articles](#)
- [Community Post - engage in discussions about GDPR](#)

And of course, we're always standing by to support you, especially as we all tackle sweeping changes like this one. If you don't succeed, we don't succeed. Please [contact us](#) if you need additional guidance or support.