HighLevel Privacy Guide for Customers

What You Need to Know About Privacy Compliance!

Last Updated August 2023

HighLevel

Privacy Laws and Regulations

Privacy laws regulate the storage and usage of personally identifiable information, personal healthcare information, and financial information of individuals that is collected by governments, public or private organizations, or other individuals. The laws may vary by country, region, territory, state, or otherwise, but there are some commonalities amongst most privacy laws in terms of the rights, obligations, and enforcement provisions.

If you collect, store, or use information that is subject to privacy regulations, then you are required to take certain steps to protect that information based on the location of the individual from whom you are collecting data. For example, if you collect personally identifiable information from your customer in the EU, you must comply with the EU's General Data Protection Regulation (GDPR). If you collect personally identifiable information from a customer in California, United States, you must comply with the California Consumer Privacy Act (CCPA), if you are subject to this law.

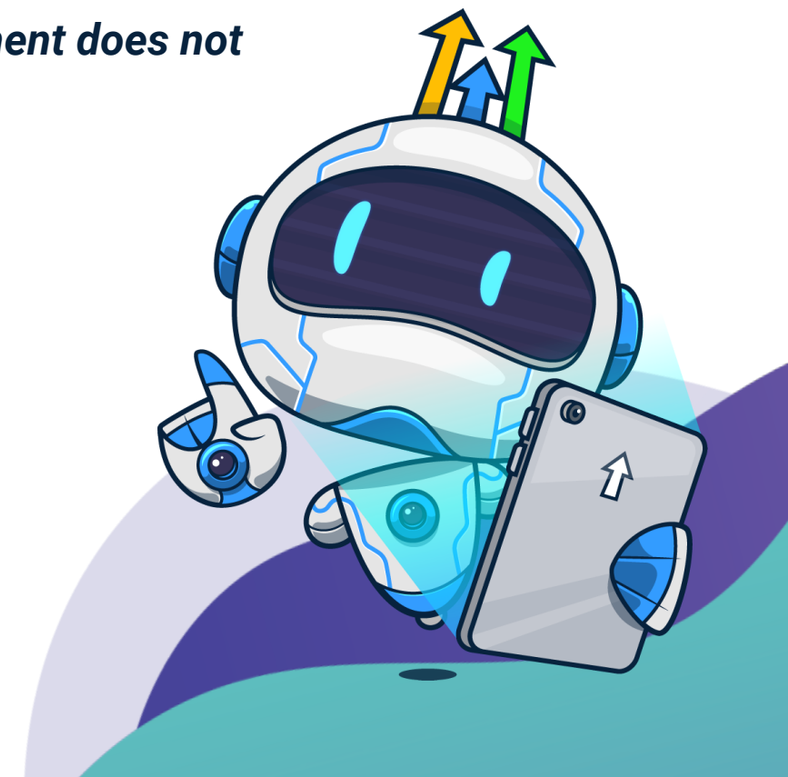
How To Use This Guide

Privacy laws and regulations are rapidly evolving, and we're going to be honest—these laws are complex! But, HighLevel wants to make it easy for our customers to stay compliant with the latest privacy laws. While HighLevel makes efforts to be compliant with privacy regulations, our customers also have to take steps to be compliant.

This guide is not meant to explain all the applicable privacy laws and regulations. It is intended to be a resource to help you use the HighLevel Platform in a way that complies with privacy requirements. That being said, our lawyer wants us to make it very clear that this document does not constitute legal advice nor is it intended to ensure compliance with privacy laws and regulations.

DISCLAIMER: HighLevel is not a licensed legal representative and cannot provide legal advice or interpret the law for you. Please consult your own legal advisor. This document does not constitute legal advice and should not be used as such.

Now, let's dive in…



Data Roles

Privacy laws impose various obligations on a person depending on whether they are a controller or a processor of personal data.

A controller is an entity which decides to process personal data, and makes decisions regarding the basis of processing and the methods which will be used. Controllers have certain obligations regarding personal data, which you should familiarize yourself with before collecting personal data from your customers.

A processor is an entity which processes data for and on behalf of a controller. They make no independent decisions regarding the data or its processing, as they only process it on behalf of the controller and must comply with all instructions given by the controller.

When you use the HighLevel Platform, you are a controller. You are in control of the data you upload to the HighLevel platform, what you do with that data, and why. As a result, you are responsible for ensuring that you have a legal basis on which to process the data, and that you do not retain the data for any longer than is necessary.

You should ensure that you understand your obligations as a controller, and update your own systems and policies to allow the lawful transfer of personal data to HighLevel. We recommend you consult your own legal counsel to ensure you fully understand your obligations as a controller. In the meantime, you can use the checklist below to get started on your compliance journey!

Controller Checklist

HighLevel makes efforts to provide our customers with the functionality they need to ensure that the HighLevel portion of your business can comply with privacy laws. Below, you will see recommended steps that you should take in your HighLevel Platform account. You'll also see recommended steps that you should take outside of your HighLevel Platform account for compliance purposes.

And just as a reminder, HighLevel is not a legal representative. The recommendations below are simply that—just suggestions! We cannot interpret the law or give you legal advice, and we recommend that you consult with your own lawyer.

By the way, this checklist is intended to cover privacy laws in general. GDPR is considered to be one of the most restrictive privacy laws, so we have tailored this checklist to reflect controller obligations under GDPR. However, as we mentioned earlier, privacy laws are rapidly evolving.

We'll do our best to update this checklist on a regular basis, but if new laws are implemented or if existing laws are modified, this list might become outdated. Again, we encourage you to consult with your own lawyer to make sure you are taking all the appropriate measures to be compliant with privacy laws! We also welcome any feedback on how we can improve the HighLevel Platform to make compliance even easier for our customers!

Privacy Law Requirement	Explanation	What You Need To Do In Your HighLevel Platform Account	What You Need To Do Outside of Your HighLevel Platform Account
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 processing their data.	You need to create a privacy notice and link to it on all webforms, landing pages, order forms, shopping carts, etc. (wherever you collect personal data). See help doc here	If you choose to collect customer data through offline methods (i.e., in person), you need to make sure your privacy notice is accessible during that interaction.

Privacy Law Requirement	Explanation	What You Need To Do In Your HighLevel Platform Account	What You Need To Do Outside of Your HighLevel Platform Account
Lawfulness of Processing	In order to process someone's data, you need to have a legal basis for doing so. A "legal basis" could be informed consent, performance of a contract, or other legitimate interests. This is where you should consult your own counsel to determine if you have a "legal basis" for processing someone's data.	Create tags to track the lawful basis or create consent checkboxes to collect express consent. See help doc here Create a regular process for removing EU contacts where you no longer have a lawful basis to process their data or if the contact withdraws their prior consent. See help docs for agencies, subaccounts, and prospects.	If you are ever audited in the future, you may need to provide records that indicate the lawful basis under which you collected your customers' information. If you collect customer information offline, be sure to keep detailed records of those collections since you won't have the records in your HighLevel Platform account.
Consent	If you want to use consent as your lawful basis to process data for a contact, there are a few requirements that you should consider: 1) You must be clear about what consent you're asking for (and make reference to your privacy notice); 2) Do not pre-check the consent checkboxes;	Update all your webforms and landing pages with consent checkboxes. See help doc here	Implement these guidelines anywhere else in your business where you ask for consent or personal information. Consider creating documentation (with a time stamp) any time you make changes to your consent checkboxes or privacy notice. This is important so that you

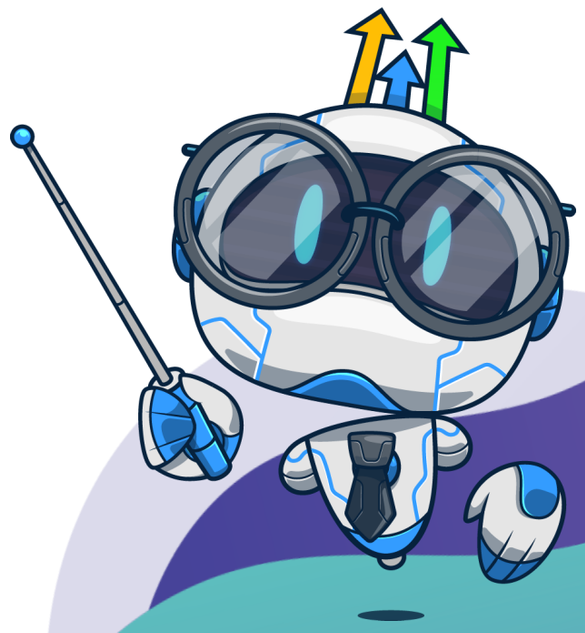
Privacy Law Requirement	Explanation	What You Need To Do In Your HighLevel Platform Account	What You Need To Do Outside of Your HighLevel Platform Account
	customers need to explicitly consent by checking the box themselves; and 3) you need to be able to show proof of consent for prospects and customers who have granted it.		can show the exact text your contacts agreed to. This information is not captured in your HighLevel account automatically.
Right to Erasure/ Delete; Right to Rectify/Correct Inaccuracies	If a person wants you to stop processing their data, they can request to be erased from your data records completely.	Create a simple way for your customers to request to be erased. For example, you can provide customers with a deletion request form that they must complete and return to you in order to request deletion—here's a template you can use. See the following help docs for how to delete data or accounts for agencies, subaccounts, and prospects.	You are responsible for carrying out your customer's request to erase their data and can do so within your HighLevel Platform 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 HighLevel, you need to erase those as well upon request.

Privacy Law Requirement	Explanation	What You Need To Do In Your HighLevel Platform Account	What You Need To Do Outside of Your HighLevel Platform Account
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.	Create a simple way for your customers to request access to the data you are processing for them. There are a few ways you can do this within HighLevel: 1) You can take a screenshot of the customer record and send it; or 2) You can export a contact's details in a CSV file and send it. See here for how to export contacts or client lists as a CSV	You're responsible for carrying out your customers' requests promptly. 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 HighLevel 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 that it is accurate. If errors exist, they have the right to request you update that information in a reasonably expedient manner.	Create a simple way for your customers to request that you update their data. You could use a request form similar to the data deletion request form template we provided above.	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 your contact information in HighLevel, 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.

Privacy Law Requirement	Explanation	What You Need To Do In Your HighLevel Platform Account	What You Need To Do Outside of Your HighLevel Platform Account
Designation of Data Protection Officer, Chief Data Security Officer, and Representatives	You may want to appoint a Data Protection Officer (DPO) or a Chief Data Security Officer for your organization. In addition, if you have customers in the EU or the UK, and have not appointed an EU or UK Data Protection Officer, you will need a representative in each region to handle any data or security dealings. There are third-party services that can serve this role for you.	Update your privacy notice to name the individuals who fulfill the EU and UK representative roles. Identify your Data Protection Officer and Chief Data Security Officer, if applicable.	Update your privacy notice to name the individuals who fulfill the EU and UK representative roles. Identify your Data Protection Officer and Chief Data Security Officer, if applicable.

More Resources

We hope this was a useful resource. Below, you will find links to other HighLevel resources and some external resources, but we can't reiterate this enough: Privacy laws are complex, and we are not lawyers, so please consult with your own legal counsel. Nothing in this document is intended to be legal advice.



HighLevel Resources:

Privacy Policy

Data Processing Agreement

Privacy and Security at HighLevel

External Resources:

GDPR EU: https://gdpr.eu/

GDPR UK: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

CCPA: https://oag.ca.gov/privacy/ccpa

Colorado Privacy Act: https://coag.gov/resources/colorado-privacy-act/

Washington My Health My Data:

https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy?