CONSENT MANAGEMENT FOR HEROKU

We can help you honor your customer's request to receive only specific forms of contact from your company. Various data protection and privacy regulations are in place to respect your customer's privacy. We provide details to help you determine the best way to comply with the data protection and privacy regulations that apply to your company.

EDITIONS

Available in: All Editions

Many data protection and privacy regulations require you and your company to honor people's requests about how you use their data. We've listed a few of the regulations that are important to many companies collecting and processing their customers' data.

- General Data Protection Regulation (GDPR), European Union
- Gramm-Leach-Bliley Act (GLB Act), United States
- Canada's Anti-Spam Law (CASL)

If you have customers or users who request specific methods of contact from your company, review this common request and the related procedures.

Common Customer Request	Actions to Consider	Things to Consider
I want to be able to request and track our users' consent to store their personal data and marketing, data processing, and data deletion preferences.	Heroku Services give you the ability to fully manage the development, design, and functionality of applications you deploy. Using Heroku Services, you can design and develop application-layer functionality that allows your organization to obtain and track consent and preferences for your application's end users.	Work with your legal team to design a consent management system that works for your specific customer needs.
I want to utilize third-party add-ons from the Heroku Elements Marketplace to store and/or manage our users' personal data.	Salesforce Heroku provides the ability for your organization to deploy third-party add-ons from the Heroku Elements Marketplace to extend and enhance capabilities of applications your organization deploys to Heroku Services.	Work with your legal team to ensure that you have the appropriate contractual terms in place with the provider of the add-on. Also make sure that you have the right processes to help manage your GDPR compliance obligations when using the add-on.
How do I minimize our users' personal data from being output to logs generated by applications our organization deploys to Heroku Services?	Salesforce Heroku aggregates logs from your application's running processes, system components, and backup services as described in the documentation into a single channel known as Heroku Logplex. Your organization can minimize transmission of sensitive data into the Heroku Logplex log stream by: • Turning off logging for your Heroku Postgres database by using the	If the Shield Private Spaces feature Private Space Logging is utilized, then logs are not stored within Heroku Services. If a third-party add-on is utilized to store logs, then your organization needs to work with the add-on provider to determine steps to minimize your users' personal data from being captured by the third-party add-on. Work with your legal team to ensure that you have the appropriate contractual terms in place with the provider of the add-on.

Common Customer Request	Actions to Consider	Things to Consider
	--block-logs option when creating the database. • Excluding such data in URLs or query strings submitted to web processes. • Not configuring application processes to print such data to stdout. Shield Private Spaces also includes the feature Private Space Logging which enables you to configure log capture at the space level instead of the app level. This feature allows your organization to forward all log events from applications and Heroku system services in the space to a single external log capture destination as described in the documentation.	Also make sure that you have the right processes to help manage your GDPR compliance obligations when using the add-on.