Email template: Contact your SaaS vendors to request better data protection and privacy

Do you have SaaS vendors who don't encrypt your data with a dedicated key? And who don't allow you to hold your own keys to keep control of your data? If they're only encrypting data at rest transparently and with a common key across their customers, then your data isn't protected on running servers.

With application-layer encryption where the data is encrypted before it's stored, the data is meaningfully protected. When you hold your own keys, you can revoke access if necessary, monitor how your data is being used, and meet data sovereignty and privacy regulations that cover your company.

Here's an email template that you can use (or start from) to ask your SaaS vendors to do better and meet industry security standards. Please copy and paste so you can make it your own.

Subject line: Options for data encryption and bring your own key (BYOK)?

Hello {insert name here},

We are reviewing the security practices of our SaaS vendors, and I have a few questions to ask either you or a colleague of yours with relevant product security knowledge.

1. Is our data encrypted?
2. Is it encrypted with a different key that isn't used for your other customers?
3. Is the data encrypted before it's sent to a data store (or is it only encrypted at a disk or database level)?
4. Is there an option for us to hold our own key?

This is important to us for a few reasons. First, we want to make sure that our data isn't available for bulk scraping along with your other customers in the case of a breach. Second, we want to make sure we have the right and the ability to revoke access to our data if we should have cause to do so. Third, we want to be able to monitor how our data is accessed for data governance purposes. And finally, holding our own key opens up ways for us to meet data sovereignty requirements by making access to the data subject to court orders in our country. We'll also need some contractual promises from you to ensure that this is the case.

> Given that you hold data that is sensitive for our business and subject to regulation, these questions are of great concern to us and if the answer to any of them is “no” (or if the answer is “transparent” encryption) then I’d like to discuss how you will work to better protect our data.
>
> Other vendors like you are adding this functionality and I know some have used IronCore Labs, which supports all of the above functionality through their partnership with Thales.
>
> I look forward to hearing your responses to the questions and, if necessary, to hearing from you about your roadmap to stronger encryption, data, visibility, and customer control.
>
> Thanks,
>
> {name}

If you’re having trouble copying any of this text, you can also view the document as a Google doc via this link.

About IronCore Labs

IronCore Labs is a data security platform for application-layer encryption and bring your own keys (BYOK). We enable software developers and businesses to rapidly build enterprise applications with strong data control. Data owners decide who can access their data, monitor how it’s used, when, where, and by whom, and can revoke that access at any time. IronCore Labs is the fastest and easiest way to control data in multi-cloud and SaaS environments.

IRONCORE LABS