SAAS DATA PRIVACY ™

Who Has Access to Your Information?

Smart SaaS™

Copyright © 2025 by SS Certification Association | All rights reserved.

TABLE OF CONTENTS

INTRODUCTION

PART 1

PART 2

PART 3

PART 4

PART 5

VISIT US AT

SMARTSAAS.WORKS

Copyright © 2025 by SS Certification Association | All rights reserved.

INTRODUCTION

Most people think of buying software as a straightforward transaction. You pay vendors. They provide access to their solution. **With software-as-a-service (SaaS), it's more complicated.**

Its cloud-based delivery model means you're not just giving them money. You're also giving them access to your data—raising a host of data privacy issues and potential dangers.

This eBook explores why data privacy is essential in SaaS and how you can insulate yourself from related legal, financial, and reputational risks when selecting a provider.

Copyright © 2025 by SS Certification Association | All rights reserved.

SAAS DATA PRIVACY

SAAS DATA PRIVACY AND WHY IT MATTERS

Data privacy focuses on who has access to data and how it is used. While closely related to data security, data privacy is a distinct concept involving:

- Ensuring users control their data, including how it's collected, processed, and accessed
- User consent for data collection and processing
- Policies on data sharing, retention, and deletion
- Compliance with privacy regulations (e.g., GDPR, CCPA, HIPAA)

	Data Privacy	Data Security
Focus	Who collects/accesses data and why	How data is protected from threats (internal/external)
Key Concern	Compliance, user rights, ownership, and transparency	Protection against data loss, breaches, and hacking
Measures	Policies, contractual agreements, access controls	Encryption, authentication, access controls, and monitoring

Keep in mind that a provider could have excellent security protocols—encryption, firewalls, detection—but violate privacy by misusing customer data. Conversely, a vendor could have great privacy policies but poor security that leaves you vulnerable to breaches.

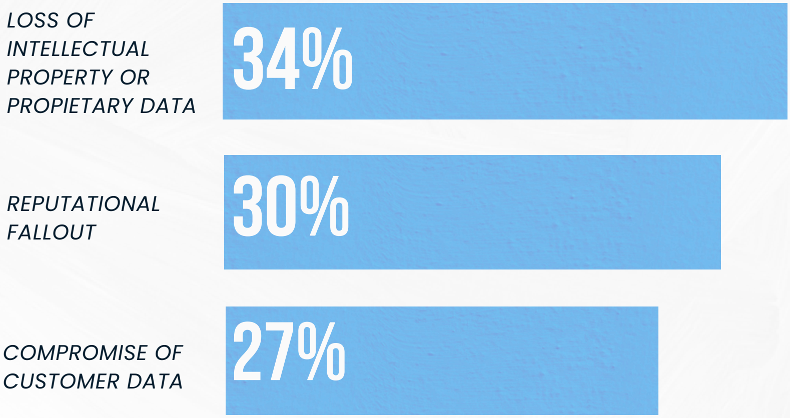
Copyright © 2025 by SS Certification Association | All rights reserved.

SaaS solutions often handle vast amounts of business and customer data. Before you sign, consider SaaS vendors' approaches to privacy and security.

REAL WORLD EXAMPE : ZOOM SETTLES PRIVACY LAWSUIT FOR $85 MILLION

A class action suit alleged that Zoom shared personal data with Facebook, Google, and LinkedIn without user permission. In the settlement agreement, Zoom agreed to pay $85 million, increase security, and alert users about third-party app data sharing. ***(NPR)***

CONCERNS AROUND SAAS SECURITY APPLICATIONS



Source: helpnetsecurity.com

Copyright © 2025 by SS Certification Association | All rights reserved.

KEY CONCEPTS

REGULATORY FUNDAMENTALS

Legal requirements for data privacy often kick in based on:

- The type of data you’re collecting and storing
- Industry-specific regulations
- Where your business is located
- Where your customers reside

If your company operates globally or even across one or two regions, it’s vital to work with your legal, IT, and compliance teams to navigate what’s become a complex web of regulatory rules.

1. DATA ACCESS

The Principle of Least Privilege (PoLP), also known as minimum access policy, dictates that users and applications should only have the minimum level of access necessary to perform their job. Taking that approach minimizes risks of unauthorized access and data breaches, and, in many cases, it’s needed to fulfill requirements for privacy laws like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

Ensure your SaaS provider can deliver the appropriate data access control features based on the granularity you need—role-based (RBAC), attribute-based (ABAC), or fine-grained access control.

Copyright © 2025 by SS Certification Association | All rights reserved.

2. DATA SOVEREIGNTY

Data sovereignty dictates which country or jurisdiction has the authority to oversee and control data generated within its borders. It encompasses regulating data collection, storage, processing, and distribution.

3. DATA LOCALIZATION/RESIDENCY

Data residency is the physical location where data is stored. Data localization refers to storing data within the jurisdiction where it was collected. Cloud providers offering data residency options can help organizations meet data sovereignty requirements by ensuring data is stored and processed in specific regions or jurisdictions.

4. REAL-WORLD EXAMPLE: ASANA'S APPROACH TO DATA RESIDENCY

Asana is a project management solution. The company provides users with multiple options for data residency and data backup regions. However, Asana only offers these options to its Enterprise and Enterprise+ plans. The company also limits customers to storing data in a single region. ***(Asana)***

UNLOCK THE SECRETS OF SAAS SECURITY

Dive deeper into the world of SaaS protection with our free eBook, SaaS Security Unmasked. Discover practical strategies, expert insights, and key steps to safeguard your cloud applications.

Download your copy now and stay ahead of threats.

Copyright © 2025 by SS Certification Association | All rights reserved.

DATA OWNERSHIP & CONTROL

Data ownership dictates who owns the data stored on a SaaS platform. Most providers have language that says the users/customers “own” their data. But don’t be fooled by simple statements about ownership. Dive deeper to ensure you control your information and how it’s used.

1. DATA PORTABILITY

Data residency is the physical location where data is stored. Data localization refers to storing data within the jurisdiction where it was collected. Cloud providers offering data residency options can help organizations meet data sovereignty requirements by ensuring data is stored and processed in specific regions or jurisdictions.

2. DATA RETENTION & DELETION

When it comes to data retention and deletion, there are two primary concerns. You want to ensure your SaaS provider won’t prematurely erase data that you need to operate your business—such as part of an automated process to reduce database size or if you terminate your contract with them. Conversely, you also want the ability to permanently delete data as needed to comply with regulations like GDPR and, again, if you terminate your relationship with the vendor.

3. REAL-WORLD EXAMPLE: WORKDAY’S APPROACH TO PORTABILITY

Workday **privacy policy** indicates the company’s commitment to “complete transparency regarding how their data is returned, transferred, and deleted if the agreement comes to an end” as part of its ISO 27018 certification. Workday reiterates this in a **Universal Data Processing exhibit** but doesn’t specify format, timelines, etc. Be sure to ask clarifying questions of any SaaS provider to avoid getting locked in with a vendor.

Copyright © 2025 by SS Certification Association | All rights reserved.

REAL-WORLD EXAMPLE: ASANA'S DATA DELETION POLICY

Asana's **data retention policy** includes provisions for deleting "inactive work data." Projects or tasks that meet the company's definition of "inactive" are trashed in weekly batches and then permanently removed after 30 days if not recovered by users proactively. This approach may fit your business needs, but Asana's policy highlights the importance of understanding SaaS providers' policies for retaining and deleting user data.

TAKE BACK CONTROL: SAAS DATA OWNERSHIP AND PORTABILITY

Avoid getting locked into a single vendor. ***Explore SaaS Data Ownership and Portability: Don't Be a Vendor Hostage to*** understand your rights, ensure data accessibility, and maintain business agility. Learn more in the full guide.

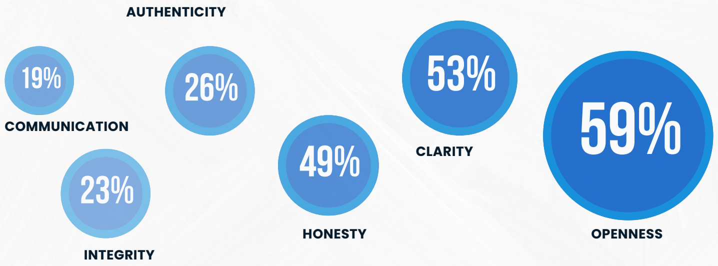
Smart SaaS
SaaS Data
SaaS Data Ownership and Portability: Don't be a Vendor Hostage

Copyright © 2025 by SS Certification Association | All rights reserved.

TRANSPARENCY IN USING, SHARING, SELLING DATA

There are many legitimate reasons that a SaaS vendor might use or share your data…and then there are others. The key is to find SaaS providers that offer clear and transparent policies about their approaches and give you easy opportunities to opt out if needed.

HOW CONSUMERS DEFINE TRANSPARENCY?



Source: sproutsocial.com

1. SAAS PROVIDER DATA USE

Great SaaS providers always look for ways to enhance their solutions and offerings. They capture in-app analytics that demonstrate how users interact with their software to understand how to improve usability and prioritize investments for new features and functionality. However, SaaS solutions often use that same data for upsells and cross-sells to drive expansion revenue.

2. THIRD-PARTY SHARING

There are many legitimate reasons that a SaaS vendor might use or share your data…and then there are others. The key is to find SaaS providers that offer clear and transparent policies about their approaches and give you easy opportunities to opt out if needed.

Copyright © 2025 by SS Certification Association | All rights reserved.

3. "SELLING" USER DATA

You'd be hard-pressed to find a privacy policy or other legal document from a SaaS provider that explicitly says, "We sell your data." In fact, most say that they don't. The tricky part of these disclaimers is how "sell" is defined in the company's jurisdiction. For example, the US defines "selling" personal information as exchanging personal data for monetary gain or other value. Not "selling" data doesn't eliminate the possibility of a vendor "sharing" it for use in targeted advertising or marketing purposes.

REAL-WORLD EXAMPLE: SHOPIFY'S "WE DON'T 'SELL' YOUR PERSONAL INFORMATION" STATEMENT

Like many companies, **Shopfiy's privacy policy** includes a statement to assuage customers' concerns about their data being sold.

"We do not "sell" your personal information as that term is defined under US Privacy Laws."

Yet Shopify explicitly lists advertisers and marketing vendors as "recipients of personal information," and the type of "personal information" the company collects and shares is extensive.

It's hard to decipher from the **merchant privacy policy** if **merchant customer data** is included/excluded in data sharing—underscoring the need for your legal team to review vendors' policies and terms.

Copyright © 2025 by SS Certification Association | All rights reserved.

THE SHARED RESPONSIBILITY MODEL

ABOUT THE SHARED RESPONSIBILITY MODEL FOR SAAS

The shared responsibility model in SaaS outlines the responsibilities that both a SaaS provider and you, its customer, need to do to ensure data privacy. This framework is designed to clarify who is accountable for securing which aspects of the platform and the data housed inside.

Most laws around data privacy and software distinguish between who in the relationship is the data controller or the data processor depending on the information at issue—your company's data, your customers' data, who's using it, and how it's being used.

It gets complicated quickly and typically requires privacy/legal expertise if your business operates in multiple locations. That said, here are some guidelines:

SaaS Provider Responsibilities	SaaS Customer Responsibilities
• Securing the platform, infrastructure and databases from breaches • Offering privacy-focused features, such as access control and data masking • Ensuring compliance with industry regulations related to data residency and localization • Earning and maintaining required privacy and security certifications (e.g., SOC, ISO) • Providing transparent data privacy policies • Sharing best practices with users/customers	• Vetting providers for the appropriate privacy policies and functionality • Ensuring contracts define ownership and handling of data • Configuring privacy settings properly (e.g., role-based access, encryption settings) • Establishing internal privacy policies • Training employees on data privacy best practices • Managing and minimizing data collection within the SaaS platform

Copyright © 2025 by SS Certification Association | All rights reserved.

CHOOSING A SAAS PROVIDER

KEY QUESTIONS WHEN CHOOSING A SAAS PROVIDER

It's critical to carefully review SaaS providers' privacy policies, terms of service, master service agreements, and other legal documents. The type of software and data housed within will dictate the importance of privacy controls and questions to ask.

What questions to ask a SaaS provider?
Who owns the data stored in the SaaS platform?
How can customers export or delete data if we switch providers?
What privacy measures does the vendor provide to protect data?
Has the provider earned industry-standard compliance (e.g., SOC and ISO)?
Where does the vendor physically store data, and what data sovereignty/privacy laws apply?
Is the provider compliant with relevant privacy laws (GDPR, CCPA, etc.)?
Does the provider monetize user/customer data? If so, how?
Does the provider share data with third parties? If so, why and how?

Copyright © 2025 by SS Certification Association | All rights reserved.

STAY PROACTIVE WITH PRIVACY

Requirements for regulatory compliance have often driven how companies think about and prioritize data privacy. But the reality is that businesses need to be equally worried about protecting their data and what can be gleaned from it to keep a competitive edge. As you consider new and existing SaaS relationships, dig into who owns the data, where it's stored, how it's used, and how it's protected. While it's prudent to emphasize enterprise-wide software solutions with hefty price tags, "free" platforms can introduce potential costs and risks that far exceed their price tags.

Engaging your IT, legal, privacy, and compliance teams in SaaS purchases is the safest course, but at a minimum, provide guidelines that empower employees to make Smart SaaS™ decisions.

READY TO LEARN MORE?

SAAS SECURITY UNMASKED

Hidden Risks You Might Overlook

Smart SaaS

SaaS Security Unmasked™

Download your copy now and stay ahead of threats.

DON'T GET SAAS'D™

B2B Buyer's Guide to Healthy Software Partnerships

Smart SaaS

Don't Get SaaS'd™

Stay empowered, informed, and in control.

Join the Conversation

Follow us in ▶ X

Check Out Additional Resources

Copyright © 2025 by SS Certification Association | All rights reserved.