Trust at Sprinklr
Data Privacy
Compliance Overview

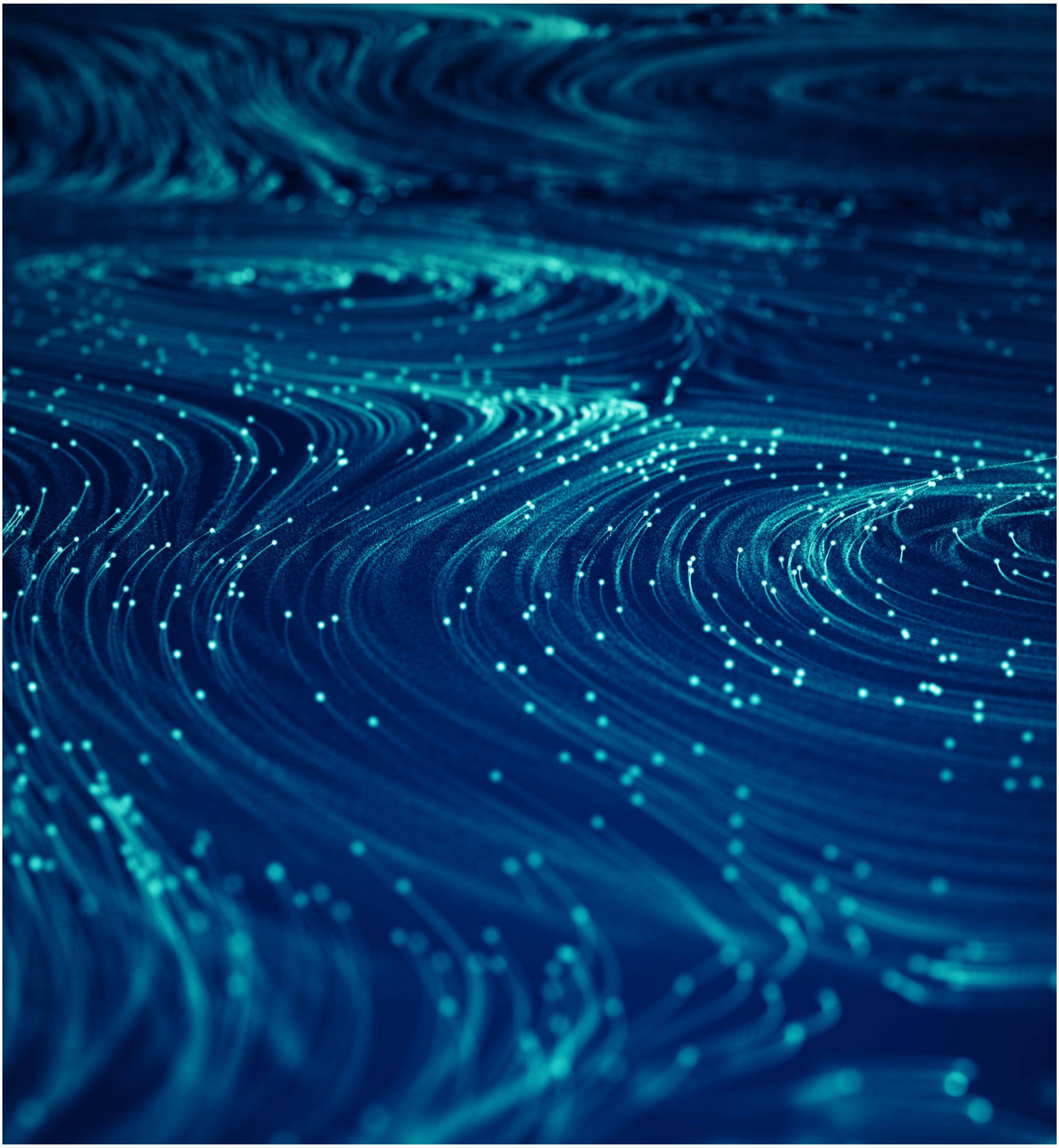
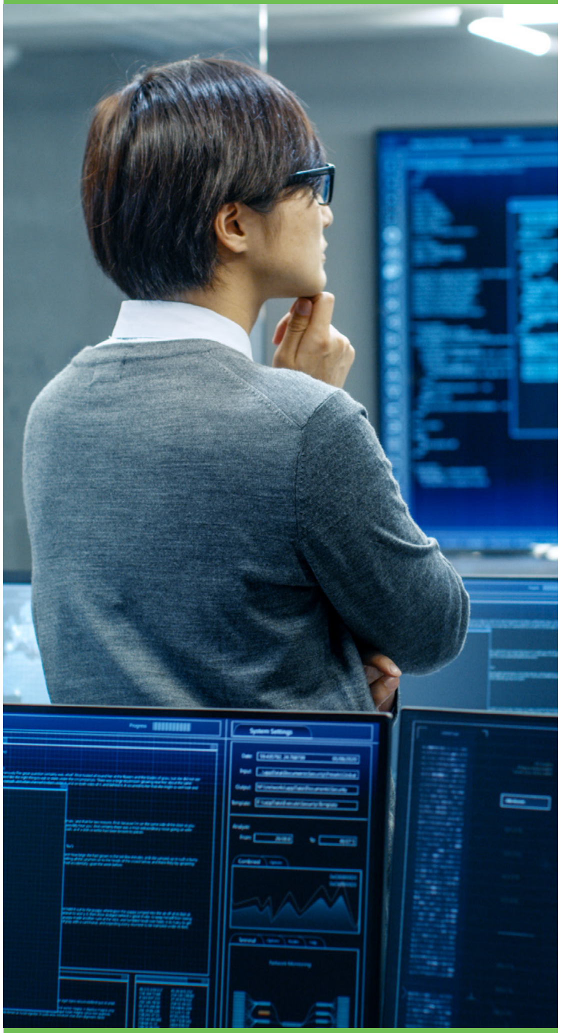


Table of contents



Your Privacy Matters

At Sprinklr, trust is integral to our business model. It underpins our core values and is crucial to how we operate. Trust is about partnership and collaboration with our customers.

Ensuring the privacy of customer data is a critical part of how we build trust at Sprinklr. As a service provider and data processor for our customers, Sprinklr is committed to supporting customers in their compliance with data privacy requirements.

Data Privacy and security are part of our culture, values, and everyday conduct at Sprinklr. We embed privacy at the design phase, right through the development lifecycle of our products and beyond.

Sprinklr's Guiding Privacy Principles

We have guiding privacy principles that are set out in our internal Data Privacy Policy, which govern how we process personal data at Sprinklr:

- We process personal data in a way that is **fair, lawful and transparent**
- We **respect the rights and requests of individuals** when processing personal data
- We process personal data on behalf of our customers for **specified and limited purposes**
- We only process the personal data **necessary to achieve the specific purpose**
- We ensure personal data can be kept **accurate and up to date**
- We enable **data retention practices** so that data is not retained for longer than necessary to achieve the processing purpose
- We implement **measures to secure and safeguard personal data**
- We are **accountable and responsible** for our personal data processing

This overview is intended to provide our customers and partners with key information about Sprinklr's data privacy program. You can also find additional details about Sprinklr's privacy and security program, as well as access to our certifications and other documentation, on our Trust Center.

Sprinklr's Management of Data Privacy

Sprinklr sees privacy as fundamental to its services, and is committed to supporting our customers in their compliance with data privacy requirements. Our legal and compliance team, in partnership with our security and product teams, closely monitors evolving data privacy laws and manages and supports Sprinklr's ongoing compliance with applicable laws (GDPR, CCPA/CPRA, LGPD, etc.).

A Dedicated Data Privacy Team

Sprinklr has a dedicated internal privacy team, with an externally appointed Data Privacy Officer, to ensure independence, rigor, and integrity. Sprinklr's privacy team supports all business functions in the assessment of privacy requirements across our products and business practices. In our Privacy Notice, you can find more information about Sprinklr's Data Privacy Officer and how to contact Sprinklr's privacy team.

Internal Governance

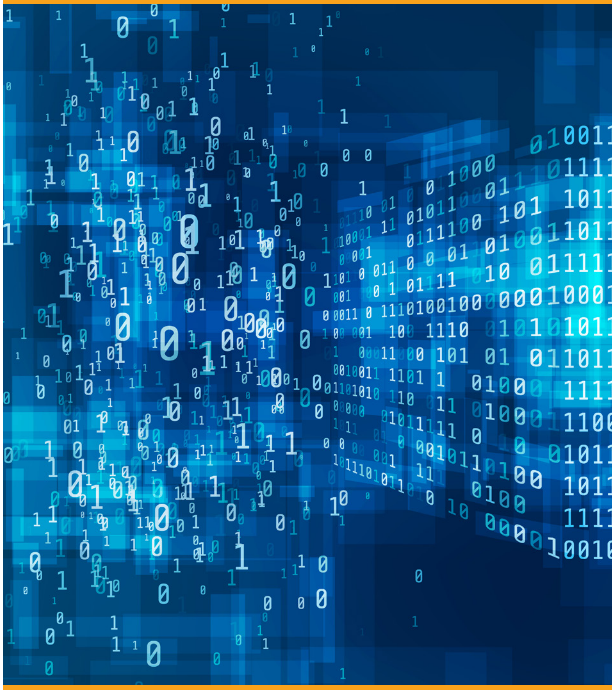
We have a robust suite of policies and guidance with regard to personal data processing at Sprinklr, which are enabled by Sprinklr's internal Data Privacy Policy. That policy implements our commitment to data privacy and provides guidance and reference material to educate and support our colleagues and ensure we do the right thing.

Global Lens

We are a global organization with people and systems all over the world. We regularly horizon-scan to understand the applicability of regional privacy laws to Sprinklr. We adopt a principles-based approach to data privacy to capture the key requirements of applicable privacy laws across the world.

Training

Sprinklr is committed to ensuring all of our employees understand their obligations under applicable data privacy laws. All employees are required to treat customer data as confidential data, and all new hires that join Sprinklr are trained on privacy and security during onboarding. Sprinklr also conducts annual refresher training, as well as tailored training for specific teams, throughout the year.



Sprinklr Products and Data Processing

The Sprinklr platform is a cloud-based SaaS application that is provided over the internet in a multi-tenant, third party hosted environment. Sprinklr offer a complete enterprise customer experience platform that is built to help our customers create and optimize valuable social experiences for their customers as well as the ability to manage customer care.

Sprinklr's Platform

Sprinklr Marketing: allows customers to manage their advertising programs through campaign automation and optimization. Sprinklr's platform enables the consolidation of advertising campaigns at its customer's instructions.

Sprinklr Service: analyzes and streamlines customer care by integrating third-party communication channels in one unified platform. Our unique AI capabilities enable our customers to appropriately prioritize and engage with individuals while gaining valuable insights into agent performance and customer engagement.

Sprinklr Insights: uses AI to turn unstructured publicly available data into actionable insights, whether this is data about certain topics, competitors, or our customers' brands.

Sprinklr Social: offers streamlined social media management, allowing monitoring and engagement with all social media channels through a unified platform.

Sprinklr Processes Personal Data on Behalf of Customers

As a processor and service provider for our customers, Sprinklr processes customer data only as needed to provide its services. Our customers are the controllers of their personal data, and we only process it in accordance with their instructions.

Sprinklr serves as the controller only for certain limited data processing activities with our customers, such as processing business contact information, billing information, marketing preferences and login credentials, so we can provide you with our service and manage the relationship with you. For more information on the personal data we process as a data controller, please click here.

Data Processed by Sprinklr

To provide its products and services to its customers, Sprinklr processes the following personal data types in its capacity as a service provider, and processor:

Account Information: this includes personal data such as identification data (name, login), contact information (business email address), work-related information (job title or role), social information (social contact handling data), and usage information (performance data, device data, and location data). This personal data is processed to manage our relationship with our customers and provide, develop, support and improve our products and services.

Inbound Content: this includes personal data published or sent by third parties (e.g., social media users) via the channels integrated with the platform, including customers' social media profiles, as well as publicly accessible data from the social media networks or other websites used for social and content management and research capabilities. Inbound Content may include user IDs, social network profile names and information, social network communications (both public and private messages to customers), as well as information shared across social media networks and other websites, such as comments, reviews, reactions and engagement. To receive Inbound Content, Sprinklr integrates with a number of third-party data sources via APIs.

Data Sources for Inbound Content: For Sprinklr Marketing, Service, and Social, the personal data is received through direct integration and authentication of these third-party channels by our customer end users. For Sprinklr Insight, the personal data received and processed in each customer's Sprinklr instance is dependent on the searches, queries, and keywords run by our customer end users against social media channels, news sources, blogs, forums, or review sites.

Customer Care Data: this includes personal data submitted by our customers' customers, followers, fans and other individuals to our customers through Sprinklr Service for purposes of customer care and support (including, where applicable under the relevant order form, voice data).

Customer Content: this includes any other category of personal data a customer provides.

Sprinklr does not request or require special categories of personal data in order to provide our services to our customers. Whether or not such data may be processed by Sprinklr depends on the type of data customers choose to store or load into the Sprinklr platform or the types of content social media users choose to make publicly available on social media channels or the web.

Transparency

Sprinklr believes transparency is key, not only to our business operations but also to building trust with our customers. Processing of personal data for the creation, maintenance, and management of relationships with customers or website visitors, is documented in our Privacy Notice. Sprinklr also provides a privacy request form to assess further questions about Sprinklr's processing and assist with data subject requests directed at Sprinklr.

For all other processing, Sprinklr does not interface directly with our customers' followers, end users, purchasers, or other individuals whose information may be processed on behalf of our customers on the Sprinklr platform. Each of our customers, as controllers, is responsible for ensuring they provide sufficient transparency, notice, and disclosure to their end users regarding their engagement of third parties such as Sprinklr; and the services that Sprinklr has been retained to provide. For more information, please refer to Sprinklr's Acceptable Use Policy.

Enabling Compliance with Data Privacy Requirements

Sprinklr processes personal data on the instruction of our customers and enables customer compliance with global data privacy laws:

Comprehensive Data Processing Addendum

Sprinklr's Data Processing Addendum (DPA) complies with applicable legal and regulatory requirements, places obligations on Sprinklr as a data processor and service provider, and gives our customers rights over the personal data we process for them. Specifically, Sprinklr's DPA:

Is tailored to Sprinklr's service and processing activities and captures the types of data processed by Sprinklr, as well as the processing activities performed by Sprinklr, in the provision of our services. Our multi-tenant SaaS architecture and unique product offering does not lend itself to bespoke agreements. Our DPA is drafted with a global lens and captures the key requirements imposed on Sprinklr as our customers' service provider and processor. Our DPA also captures the required transfer mechanisms to enable cross-border data flows and details the enterprise-wide security commitments Sprinklr employs to further safeguard customer data.

Defines Sprinklr as a Processor and Service Provider, and in this role, Sprinklr only acts in accordance with our customers' documented instructions.

Commits to supporting customer privacy assessments such as Data Privacy Impact Assessments for high risk processing activities or supporting the execution of data subject requests.

Requires prompt notification of security incidents impacting customer data, including 48-hour notice of such incidents and ongoing support for the investigation and remediation of any incidents.

Requires deletion of data upon customer request, in accordance with customer-selected and configured data retention schedules, or upon the termination of the relationship. Details of retention packages available are set out in our SLA.

Provides customers with audit rights so that our customers can monitor our legal and contractual compliance. All audits must be completed in accordance with Sprinklr's policies and requirements for on-site and virtual audits.

International Transfers

Because most of Sprinklr's customers are global organizations with customers located all over the world, Sprinklr's DPA anticipates the need for cross-border data transfer safeguards. Our DPA leverages the most up-to-date EU Standard Contractual Clauses and the UK Data Transfer Addendum to safeguard data transfers from the EEA or UK to third countries. You can refer to Sprinklr's White Paper on International Transfers for more information about Sprinklr's approach to restricted transfers and all details needed to require a Data Transfer Impact Assessment.

Sprinklr's Approach to Requests for Personal Data from Public Authorities

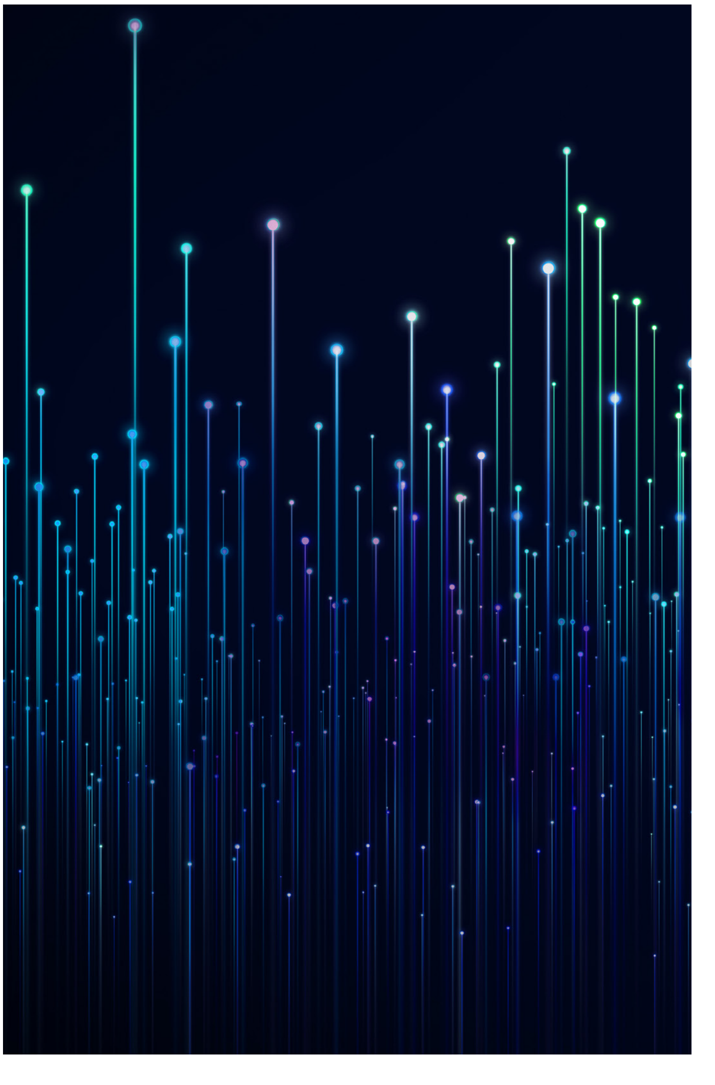
Sprinklr's legal team monitors and review all requests for information received by Sprinklr, including requests from governments or third parties. In the event Sprinklr receives any request for customer data from public authorities, Sprinklr's legal team will carefully assess such a request and first inform authorities that they should request the data directly from the customer. As legally permitted, Sprinklr will also use commercially reasonable efforts to inform customers of the circumstances of the required disclosure.

In circumstances where Sprinklr is required, under applicable law, to allow access to customer personal data, Sprinklr's legal team will assess the lawfulness and proportionality of such requests and make commercially reasonable efforts to narrow the scope and object to the disclosure as permitted under applicable law. Sprinklr will provide notice to customers as soon as legal prohibitions on disclosure are lifted.

Subprocessor Support for the Sprinklr Platform

As a global SaaS business, Sprinklr uses subprocessors across the world to help provide the Sprinklr platform, such as our global affiliates, cloud hosting solutions, subprocessors that support or enable certain product capabilities, and third parties that provide implementation and management support. Sprinklr's privacy and security teams carry out robust due diligence of subprocessors prior to engagement and periodically during the course of the relationship. Subprocessors must enter into security, privacy, and confidentiality terms that are at least as restrictive as those in Sprinklr's DPA, including a limit on their access to customer data only as needed to perform the services they are contracted for.

Our full list of subprocessors and their processing locations can be accessed here. We notify our customers of changes to this list and give them the opportunity to make reasonable objections.



Privacy & Security on the Sprinklr Platform

Privacy by Design

Sprinklr takes a privacy-by-design approach to its general business model and data processing activities. All employees are trained on data privacy. Sprinklr's privacy team regularly collaborates with all teams on privacy requirements and best practices. Technical and organizational measures are put in place during product review and development, including API configurations, masking techniques and other features to ensure a privacy-forward approach.

In-Product Privacy Center

In light of the operational burdens created by the management of data subject requests, Sprinklr puts customers in control through our **in-product Privacy Center**. Using the Privacy Center, customers can manage their data subject requests in real time, such as access, deletion and rectification.

Security Requirements

Sprinklr has a robust information security program, as outlined in the Enterprise Security Addendum within Sprinklr's DPA:

Infrastructure security: Sprinklr's production environment is completely virtual, running in an Infrastructure-as-a-Service (IaaS) third-party cloud environment. Sprinklr partners with AWS, Microsoft, and Google data centers for data hosting and leverages additional IaaS providers' security controls.

Network security: Sprinklr has implemented both reactive and proactive network security controls. We monitor network activity for anomalies 24/7 and respond to security events.

Detection & response: Sprinklr's dedicated Detection & Response team focuses on threat detection engineering, vulnerability management, incident response and crisis management to support our customers should a security incident occur.

Secure life cycle development process: Our platform is developed internally by Sprinklr employees who receive regular training on secure coding practices. Our security team works closely with engineering to inject security at every step of the development process. Sprinklr follows the Open Web Application Security Project (OWASP) guidelines and other industry-standard control systems for application security.

Encryption: Data at rest and data in transit are encrypted by default.

Sprinklr also offers a number of features and supports industry-standard controls to help protect your data and brand. These include role-based access controls, two-factor authentication, single sign-on (SSO) and IP restrictions.

Sprinklr is regularly audited by third-party assessors, evaluating internal controls that protect the security, confidentiality, and availability of the information entrusted to us by our customers. Sprinklr maintains SOC1 Type II, SOC2 Type II, PCI-DSS (for LiveChat only), ISO 27001 certifications and FedRAMP Li-SaaS authorization.

Customers can find more information about Sprinklr's security program, including access to Sprinklr's certifications and reports, at our Trust Center.

Get in Touch

If you have any questions about the processing of personal data at Sprinklr, you can contact us at privacy@sprinklr.com. We would love to hear from you.

Useful Resources

- Data Processing Agreement
- Retention Packages
- Privacy Notice
- White Paper on International Transfers
- Trust Center
- Privacy Shield Certification
- ISO 27001 Certification
- SOC Certification
- Cyber Insurance
- DPO Appointment
- Individual rights, privacy or security request
- Platform overview