General Data Protection Regulation Compliance Overview

HOW SPRINKLR TACKLES THE UPCOMING CHANGES IN DATA PROTECTION LAW
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>Data Protection Is More Important Than Ever</td>
</tr>
<tr>
<td>04</td>
<td>What Is the Sprinklr Platform Doing?</td>
</tr>
<tr>
<td>05</td>
<td>Legal Basis of Social Media Listening</td>
</tr>
<tr>
<td>06</td>
<td>Data Subjects’ Rights</td>
</tr>
<tr>
<td>07</td>
<td>International Data Protection</td>
</tr>
<tr>
<td>08</td>
<td>Data Protection</td>
</tr>
<tr>
<td>09</td>
<td>Data Security</td>
</tr>
<tr>
<td>10</td>
<td>Data Protection Team</td>
</tr>
</tbody>
</table>
Data Protection Is More Important Than Ever

Data protection and information security are part of the culture, values and everyday conduct at Sprinklr. Sprinklr's commitment to unimpeachable information security and privacy compliance builds the basis of strong and long-lasting customer relationships.

MOST IMPORTANT MESSAGE AT THE VERY BEGINNING:
All Sprinklr products and services will comply with the EU General Data Protection Regulation (GDPR), when it becomes enforceable on May 25, 2018.

In addition to our own compliance, Sprinklr is also committed to supporting our customers in their implementation of GDPR and to help them comply with GDPR requirements in connection with their usage of the Sprinklr platform and related services. This GDPR Compliance Overview intends to provide background information on Sprinklr's general compliance with data protection laws, and on Sprinklr's implementation of GDPR.
What Is the Sprinklr Platform Doing?

Sprinklr offers the world’s most complete enterprise customer experience management system, built to help large brands create, manage, and optimize valuable social experiences for their customers, across 23+ social channels and brand websites. The Sprinklr platform is a cloud based Software as a Service (“SaaS”) application provided over the Internet, in a multi-tenant hosted environment.

WHAT KIND OF DATA IS PROCESSED BY SPRINKLR?
The data and information collected and processed by Sprinklr in the context of the provisioning of the Sprinklr platform and services for our customers includes the following categories:

Account Information
- Personal data related to the customer’s employees using the Sprinklr platform required for the usage of the platform

Customer Content
- Content to be published to customer’s social media profiles (e.g. Facebook page) connected to the Sprinklr platform, uploaded by the customer (e.g. logos, brand images, templates etc.)
- For specific use cases (e.g. audience marketing) data related to customer’s customers, newsletter subscribers etc., uploaded by the customer

Social Data
- Content published or sent by social media users via customer’s social media profiles (e.g. Facebook page), connected to the Sprinklr platform (both public and private messages to customer)
- Publicly accessible data from the social media networks based on certain search queries (e.g. #customer), defined by the customer
Legal Basis of Social Media Listening

Collection of publicly accessible data from the social media networks usually is based on “legitimate interest” (and not on the social media users’ consent). The concept of “legitimate interest” and the associated balancing of interests are regulated under Art. 6 (f) GDPR. Sprinklr sees no relevant changes in the legal foundation of such data processing operations. Sprinklr will be happy to support our customers in their balancing of interests and their documentation of the legitimate interest. Please note that Sprinklr is not a law firm and may not provide individual legal advice to our customers, but only general opinion and “food for thought”.

DATA PROCESSING AGREEMENT

Sprinklr updated its standard Data Processing Addendum (DPA) in accordance with the requirements of Art. 28 (3) GDPR. Sprinklr’s DPA is available to all Sprinklr customers at sprinklr.com/legal to help them prepare for May 2018.

Sprinklr provides a list of sub-processors, including scope and geographical location of their data processing operations, engaged by Sprinklr. The list of sub-processors is available at sprinklr.com/legal. In addition, Sprinklr implemented an information mechanism, including customers’ right to object, in case of intended changes/additions to such list of sub-processors, in accordance with Art. 28 (2) GDPR.
Data Subjects’ Rights

In the 12.2 release, Sprinklr will launch a new Privacy Centre in the Sprinklr Platform to enable our customers to comply with data subjects’ rights requests (access, rectification, deletion) real-time in a more efficient way, directly via the user interface or via API so Sprinklr can participate in company wide automated GDPR processes. In addition, Sprinklr enables our customers to monitor and manage rules governing storage around all types of data from various sources.
Sprinklr is based in the USA, but also has operations in several other countries, including Australia, Brazil, Canada, France, Germany, India, Japan, the Netherlands, Singapore, Switzerland, UAE and UK.

Sprinklr uses Amazon Web Services (AWS) and/or Microsoft Azure servers to host the Sprinklr platform and to process and store customer data. Such servers are located in the United States and/or the EU.

The EU Standard Contractual Clauses are part of Sprinklr’s Data Processing Addendum and are applicable to all data exports from the EU/EEA. In addition, Sprinklr is certified under the EU – US Privacy Shield.
Data Protection

IMPACT ASSESSMENT
Sprinklr provides detailed support and all information required by our customers to enable them to perform any required Data Protection Impact Assessments, in compliance with Art. 35 GDPR.

BY DESIGN
Sprinklr ensures that data protection principles are taken into account and implemented by default throughout the development and engineering process and that the Sprinklr Data Protection Team is an integral part of the development process and will be involved in any roadmap decisions going forward.

TRAINING
Sprinklr ensures that every employee is aware of his/her data protection and confidentiality obligations. Every employee participates in mandatory data protection and information security trainings and is formally obliged to data secrecy.
Data Security

Art. 32 GDPR requires provisioning of appropriate technical and organizational security measures and a general description of such implemented security measures.

The Sprinklr platform is a multi-tenant Software-as-a-Service (SaaS) product, which is hosted in a private virtual cloud (PVC). This means that customer data shares the physical environment with other Sprinklr customers but is logically isolated to ensure security. This hosting environment creates a high availability redundant enterprise grade installation with strong security. Sprinklr normally doesn’t involve highly sensitive data requiring the associated high security, instead Sprinklr typically deals with social media posts for social media networks, including, but not limited to Facebook, Twitter, and Instagram. For these reasons Sprinklr is not PCI/DSS or HIPPA certified but Sprinklr does hold a SOC 2 Type 2 security certification.

Sprinklr’s information security program is documented in the Sprinklr Security Manual, providing a detailed overview of Sprinklr’s security and compliance infrastructure and available upon request.

DATA BREACH NOTIFICATION
With regard to the enhanced data breach notification requirements, Sprinklr operates a documented professional incident management and response system that allows us to comply with the deadlines under Art. 33 GDPR.
Data Protection Team

Data protection compliance is of paramount importance to the Sprinklr senior management. Sprinklr established a data protection steering committee of key functional leaders throughout the company.

Sprinklr also appointed an experienced Data Protection Officer (according to Art. 37 GDPR).