smartsheet

Smartsheet and the GDPR

Purpose

From its inception, Smartsheet has maintained a strong commitment to privacy and data security for its customers. This commitment has only grown stronger with the passage of the European Union General Data Protection Privacy Regulation Law ("GDPR") as Smartsheet continues to provide global, world-class service to a growing user base.

This document is intended to give a broad overview of the GDPR and address some frequently asked questions regarding users' data and the data entered or uploaded within Smartsheet's platform. It is important to note that this document does not provide legal advice. Smartsheet recommends that you consult with a licensed attorney or legal counsel to familiarize yourself with the exact regulations that govern your specific situation.

What is the GDPR?

The GDPR is a comprehensive privacy and security law enacted by the European Union Parliament, effective from May 25, 2018. The regulation is intended to strengthen existing privacy laws governing "personal data" (any information relating to an identified or identifiable natural person, or "data subject") of European residents. The law's scope is extraterritorial, applying its reach to any entity that controls or processes the data of European residents.

How does the GDPR apply to my data within Smartsheet?

The GDPR may apply if your company is processing personal data within Smartsheet relating to European Union ("EU") residents, regardless of your physical or geographic location, or if you yourself are a EU resident. European law separates those who process data into two categories of "Controllers" (those who control the collected personal data and determine the purposes and means of the processing of personal data) and "Processors" (entities which process personal data in accordance with the written instructions of the Controllers). The GDPR applies to both categories, and the two are not mutually exclusive (i.e., an entity may be acting as both Controller and Processor depending on the data set). In its business operations and in providing its services to customers, Smartsheet can be a Controller and a Processor of Personal Data, and sometimes both at the same time. Smartsheet's role as either a Controller, Processor, or both will typically be identified in a contract related to the Processing at hand or as otherwise provided for in Smartsheet's Privacy Notice.

"Processing," as defined by the GDPR, refers to any operation or set of operations performed on personal data or sets of personal data, whether or not by any automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Smartsheet is obligated under the GDPR, and other global privacy law, in its capacity as both a Controller and Processor of personal data. As a Controller, Smartsheet respects the rights of all data subjects and outlines its practices (specifically, the type of personal data that is collected, used, and shared) in its

©2020. All Rights Reserved
Smartsheet Inc.

sales@smartsheet.com
(844) 324-2360
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet

publicly available Privacy Notice. As a Processor, Smartsheet respects the rights of data subjects and follows the guidelines below when processing personal data. Although the GDPR applies only to European residents, Smartsheet does not distinguish between users located inside or outside of the European Union and has taken a global approach to its privacy and security practices.

What obligations does Smartsheet have to customers under the GDPR?

Article V of the GDPR lays out seven fundamental rights, or privacy principles, for EU residents which Controllers and Processors must uphold at all times:

1. **Lawfulness, fairness, and transparency**: Processing must be lawful, fair, and transparent to the data subject at all times
2. **Purpose limitation**: Data must be processed according to the purpose expressed to the customer at the time of collection
3. **Data minimization**: You must collect and process only as much data as absolutely necessary for the purposes specified
4. **Accuracy**: You must keep personal data accurate and up to date
5. **Storage limitation**: You may store relevant data only for as long as its specified purpose
6. **Integrity and confidentiality**: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality
7. **Accountability**: The data controller (i.e. Smartsheet customer) is responsible for being able to demonstrate GDPR compliance with all these principles

As a Controller and/or Processor, Smartsheet regularly reviews its practices to ensure that it treats all data in accordance with Article V standards. For more information on updates regarding Smartsheet's data privacy practices, please see the Smartsheet Trust Center.

Rights of Individuals under the GDPR

One of the biggest changes in privacy law following the EU's passage of the GDPR was that of expanded rights for individuals. The GDPR provides expanded rights for individuals, including the rights of:

- Access
- Erasure
- Objection
- Portability
- Rectification
- Restriction
- Withdrawal of Consent

Smartsheet respects these rights for all individuals and provides an easy, efficient way to process these requests. If an end-user has any question about their data, please complete this form or email privacy@smartsheet.com to submit an inquiry.

Valid Transfer Mechanisms

Data subjects residing in the European Economic Area ("EEA") that interact with foreign companies risk their data being transferred to jurisdictions that may not have data privacy laws that provide protections equivalent to those provided in their home country. The GDPR was designed in part to combat this data

©2020. All Rights Reserved
Smartsheet Inc.

insecurity by requiring controllers and processors to implement approved "valid transfer mechanisms" when transferring or otherwise processing personal data outside the EEA. The three major methods of appropriate safeguards include: (1) Standard Contractual Clauses ("SCC"); (2) Binding Corporate Rules ("BCRs"); and (3) certification mechanisms (such as Privacy Shield).

The Standard Contractual Clauses are specific clauses approved by the EU Commision for the protection of personal data transferred between entities and are often included within agreements between data exporters and data importers. Another valid transfer mechanism, Binding Corporate Rules, offer a level of privacy assurance through internal measures of conduct adopted by a company which are subject to approval by European data protection agencies.

Recently, the European Court of Justice invalidated the EU-U.S. Privacy Shield Self Certification program — the data transfer mechanism utilized by many companies in the United States, including Smartsheet. Despite the invalidation ruling, Smartsheet continues to maintain its Privacy Shield Certification and is committed to continuing to protect personal data in accordance with the Privacy Shield Principles (more information about the Privacy Shield Principles is available here). Additionally, Smartsheet has updated its Data Protection Addendum ("DPA") to incorporate the SCC with its European customers that choose to execute a DPA to ensure there is a valid transfer mechanism in place in accordance with the GDPR.

For additional information relating to Smartsheet's Privacy Practices post-*Schrems II*, please see "International Data Transfers to Smartsheet".

Does the Smartsheet User Agreement and Data Processing Addendum take the GDPR into account?

Yes, the Smartsheet DPA and User Agreement include privacy and security provisions for the protection of customer data.

How does Smartsheet treat Customer data under the GDPR?

Smartsheet is a global company and takes the privacy of its customers very seriously. Smartsheet and its affiliates offer world-class privacy assurances compliant with applicable data privacy legislation such as the GDPR and the CCPA. Smartsheet also monitors legislation from other countries that have the potential to affect its customer base.

Occasionally, companies will also share user data with third parties for a variety of different business purposes. However, Smartsheet does not sell customer data to third parties without explicit permission from the customer, unless otherwise agreed. Vendors are beholden to Smartsheet's Vendor Privacy and Data Handling Expectations, which align with the GDPR's guidelines on data integrity and purpose limitation when conducting business. More information on how Smartsheet treats vendor policies can be found here.

Additional Information and Resources:

- Smartsheet Privacy Notice
- Smartsheet's Privacy Practices
- Smartsheet Trust Center
- Smartsheet Data Processing Addendum

©2020. All Rights Reserved
Smartsheet Inc.

sales@smartsheet.com
(844) 324-2360
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet