Transparency Report

Published: May 9, 2023

This document provides information about Salesforce's principles for handling government requests for customer data and the relevant annual figures regarding such requests.

Background

Like many other technology companies, Salesforce may on occasion receive a request from a law enforcement or other government agency seeking access to certain data, including access to data belonging to a customer. Salesforce receives relatively few government requests for customer data as a primarily B2B company. Our goal is always to protect our customers' data, while complying with applicable laws.

This document explains the principles that Salesforce follows if we receive such a request and provides information regarding the types and numbers of requests that we have received from law enforcement and other government agencies, and how we responded to them, during the period from **January 1, 2022, to December 31, 2022** (the "Covered Period"). Customers may provide this information to their supervisory authorities, if required.

The term "customer data" used in this document refers to electronic data and information submitted by or for customers to our services, as further defined in the Main Services Agreement.

Our Policies and Process

Trust is our #1 value

At Salesforce, trust is our number one value. The protection of our customers' data is paramount to us, and we safeguard that data with a robust, comprehensive, and transparent privacy and security program. Our privacy and security programs are designed to protect our customers' privacy and protect data submitted by or for our customers to our services against unauthorized access or disclosure.

Salesforce offers its customers various contractual commitments in its Main Services Agreement (including its Data Processing Addendum) which align to the principles described below. More precisely, these commitments can be found in section 8 "Government Access Requests" of Salesforce's Data Processing Addendum, clause 15 of the Standard Contractual Clauses, which form part of the Data Processing Addendum, and section 10 of Salesforce's EU and UK Processor Binding Corporate Rules. Salesforce strongly believes that these contractual protections provide customers as much legal certainty as possible in relation to compelled disclosure.

For that reason, every government request for customer data that Salesforce receives is carefully reviewed, consistent with the laws in the relevant jurisdiction(s), to ensure the requesting government agency is entitled to the data sought with the type of process utilized. Where we believe a government request for customer data is invalid or unlawful, we will try to challenge it. We aim to fully meet our legal obligations while honoring the faith that our customers place in us.

We notify an affected customer of any legally binding and valid request for its data or any direct access to customer data by a law enforcement or other government agency, unless we are explicitly prohibited from doing so by law.

Trust starts with transparency. Unless prohibited by law, Salesforce always notifies a customer when it receives a legally binding and valid request for that customer's data, including a government request. We also promptly notify a customer if we become aware of any direct access by a government agency to customer data, and we will provide information that is available to us in this respect, to the extent permitted by law.

Where possible, we refer the requesting government agency to the affected customer.

We believe our customers should have as much control as possible over their respective data. Salesforce is not the owner of our customers' data, and we strongly believe that any

government agency seeking access to customer data should address its request directly with that customer, where possible. Accordingly, if we receive a government request for customer data, unless prohibited by law, we endeavor to refer the requesting agency to the affected customer so that the customer can work with the government agency directly to respond.

We do not disclose customer data to government agencies unless compelled by law and we challenge or reject unlawful requests.

We review each government request for customer data on a case-by-case basis and only comply if and to the extent we determine the request is legally binding and valid and we are required to do so under applicable procedural rules. We do not provide government agencies with direct or unrestricted access to our customer's data. When reviewing the lawfulness of a government request, we take into account all applicable laws, including the laws of other jurisdictions. We require government agencies to follow the required legal process under applicable laws, such as issuing their request via a subpoena, court order, or search warrant. Where we believe a government request for customer data is invalid or unlawful, we try to challenge it and pursue possibilities of appeal. If we are required to disclose customer data to government agencies, we ensure the transfer is necessary and proportionate and provide the minimum amount of information possible, based on a reasonable interpretation of the request. We apply this principle equally to all government agencies (that is, whether it is a request relating to law enforcement or national security).

If prohibited by law from notifying the affected customer, we try to get that legal restriction waived.

If we receive a government agency request for data, and we are prohibited by law from notifying the affected customer, we use best efforts to request that the confidentiality requirement be waived in order for us to notify the appropriate data protection authorities. We keep a record of the actions we have taken to waive any applicable confidentiality requirements.

We do not provide any government agency with encryption keys or any other way to break encryption.

Salesforce provides options to encrypt customer data at rest and in transit. Salesforce ensures that encryption keys are securely stored and managed in accordance with industry best practice. Many of the Salesforce services provide the option for customers to create and manage their own encryption keys, or for the encryption keys to be managed through a third party provider. This allows customers to protect and control who has access to their

data.

Salesforce does not provide any government agency with encryption keys used to secure customers' data and not facilitating any other means of breaking the encryption.

We do not build backdoors into our products.
We have not purposefully created back doors or similar programming that allows access by a government agency to our services or customers' data.

Figures

Types of Legal Processes Received

The figures below represent the total numbers of various forms of government requests for customer data, or their local equivalents, received during the Covered Period from January 1, 2022, to December 31, 2022. Any requests that do not pertain to customer data are not included in these figures.

	Subpoenas[1]	Search Warrants	Court Orders[2]	Total
# Received	43	12	2	57

Requests by Country

Although Salesforce is headquartered in the U.S., we provide services in jurisdictions around the world and have a corporate presence in several countries. Salesforce complies with the law in all jurisdictions where we operate and is thus required to respond to requests in all the countries that have legal jurisdiction over our operations. When we receive requests from governments in any country, we evaluate them carefully for validity and applicability before responding.

[1] This category includes, for example, grand jury, administrative, and civil subpoenas issued by a government agency, as well as their equivalents in other jurisdictions.

[2] This category includes, for example, pen register and trap and trace orders, and orders authorized under 18 U.S.C. § 2703(d), as well as their equivalents in other jurisdictions.

The figures below represent the total number of government requests for customer data received for the Covered Period, organized by country of origin. Any requests that do not pertain to customer data are not included. Note that any potential requests made under the CLOUD Act in the U.S. are included in the figures below.

Country	Number of Requests Received
United States	53
Australia	1
The Netherlands	1
Singapore	1
Spain	1
Total Requests Received	57

Requests by Response

The figures below represent the total number of government requests for customer data received for the Covered Period, categorized by data disclosed. “Content” refers to electronic data and information that our customers submit to our services, including customer data. “Non-Content” is Confidential Information that is not customer data, as these terms are defined in the Main Services Agreement. It includes basic customer information (such as name, address, email address, billing information) and service derived and generated data.

Requests Received from Agencies Worldwide	Content Disclosed	Only Non-Content Disclosed	No Data Disclosed	Total
# of Requests	11	44	2	57
% of Total	19%	77%	4%	100%

U.S. National Security Requests

In the United States, companies are legally prohibited from disclosing the precise number of received National Security Letters (NSLs) and court orders under the Foreign Intelligence Surveillance Act (FISA). However, the USA Freedom Act enables us to report such requests (including both NSLs and FISA orders) in broad ranges, which we do below. No inferences should be drawn from the limits of the below ranges and, as previously stated, Salesforce receives relatively few government requests of any kind.

Reporting Period	Number of Requests Received
January 1, 2022 - December 31, 2022	0-249