Transparency Report

Published: May 24, 2024

This document provides information about Salesforce's principles for handling requests for Customer Confidential Information made by Public Authorities and the relevant annual figures regarding such requests.

Background

Like many other technology companies, Salesforce may on occasion receive a request from a Public Authority, as defined in Salesforce's Data Processing Addendum, seeking access to certain data, including access to Customer Confidential Information. Salesforce receives relatively few requests for Customer Confidential Information 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 Public Authorities, and how we responded to them, during the period from **January 1, 2023, to December 31, 2023** (the "Covered Period"). Customers may provide this information to their supervisory authorities, if required.

The term "Customer Confidential Information" as used in this document, includes "Customer Data" and "Confidential Information", both as 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 Customer Confidential Information 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 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 (i) section 7 "Confidentiality" of Salesforce's Main Services Agreement, (ii) 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 (iii) 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 request for Customer Confidential Information that Salesforce receives is carefully reviewed, consistent with the laws in the relevant jurisdiction(s), to ensure the requesting Public Authority is entitled to the data sought with the type of process utilized. Where we believe a request for Customer Confidential Information is invalid or unlawful, we will 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, 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 Confidential Information, including a request. Salesforce does not provide Public Authorities with direct or unrestricted access to Customer Confidential Information. If we become aware of any such intrusion, we will promptly notify the affected customer and provide any information that is available to us in this respect, to the extent permitted by law.

Where possible, we refer the requesting Public Authority 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 Customer Confidential Information, and we strongly believe that any Public Authority seeking access to any Customer Confidential Information should address its request directly with that customer, where possible. Accordingly, if we receive a request for Customer Confidential Information, if permitted by law, we refer the request to the affected customer and encourage them to work directly with the Public Authority.

We do not disclose Customer Confidential Information to Public Authorities unless compelled by law, and we challenge or reject unlawful requests.

We review each request for Customer Confidential Information 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 Public Authorities with direct or unrestricted access to our data. When reviewing the lawfulness of a request, we take into account all applicable laws, including the laws of other jurisdictions. We require Public Authorities 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 request for Customer Confidential Information is invalid or unlawful, we challenge it and pursue possibilities of appeal. If we are required to disclose Customer Confidential Information to Public Authorities, 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 Public Authorities.

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

If we receive a request for data from a Public Authority, 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 Public Authority with encryption keys or any other way to break encryption.

Salesforce provides options to encrypt data at rest and in transit. Salesforce ensures that encryption keys are securely stored and managed in accordance with industry best practices. Many 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 Public Authority with encryption keys used to secure customers' data and does not facilitate any other means of breaking the encryption.

We do not build backdoors into our products.

Salesforce does not create backdoors or similar programming that allows access by a Public Authority to our Services or our customers' data.

Figures

Types of Legal Process Received

The figures below represent the total numbers of various forms of requests for Customer Confidential Information, or their local equivalents, received during the Covered Period from January 1, 2023, to December 31, 2023. Any requests that do not pertain to Customer Confidential Information are not included in these figures.

	Subpoenas[1]	Search Warrants	Court Orders[2]	Total
# Received	74	22	8	104

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.

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

---

[1] This category includes, for example, grand jury, administrative, and civil subpoenas issued by a Public Authority, 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.

Country	Number of Requests Received
United States	98
France	1
Germany	1
The Netherlands	2
Spain	1
United Kingdom	1
Total Requests Received	104

Requests by Response

The figures below represent the total number of requests for Customer Confidential Information received for the Covered Period, categorized by data disclosed.

"Content" refers to "Content" under The Stored Communications Act, 18 U.S.C. §§ 1701, *et seq*. ("SCA"), and includes electronic data and information, including user generated data, that our customers submit to our Services.

"Non-Content" refers to "Non-Content" under the SCA, and includes basic customer information (such as name, address, email address, billing information), as well as service derived and generated data. Non-Content can include "Confidential Information" as defined in the Main Services Agreement, but does not include "Content" as defined in The SCA.

Requests Received from Agencies Worldwide	Content and Non-Content Disclosed	Only Non-Content Disclosed	No Data Disclosed	Total
# of Requests	21	74	9	104
% of Total	20%	71%	9%	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 requests of any kind.

Reporting Period	Number of Requests Received
January 1, 2023 - December 31, 2023	0-249