UPDATED SEPTEMBER 2023

This document is provided for informational purposes. It is not intended to provide legal advice. Salesforce urges its customers to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situations. This information is provided as of the date of document publication and may not account for changes after the date of publication.

Salesforce Transfer Impact Assessment Whitepaper

Introduction: How to Use This Document

Trust is our number 1 value and nothing is more important than the privacy and security of our Customers' data. We will always protect our Customers' data, while complying with applicable laws. We see Customer compliance as a shared responsibility between Salesforce and its Customers.

The purpose of this document is to help Customers perform their own transfer impact assessment with regard to their use of the Salesforce Services, as defined in the Trust and Compliance Documentation, for transfers made under Article 46 transfer tools, including standard contractual clauses or binding corporate rules. This document (i) summarizes how Customers can use the Salesforce Services to transfer their data in compliance with European law, (ii) describes the the industry-leading contractual, technical and organizational frameworks and safeguards taken by Salesforce to ensure that an equivalent level of protection exists for Personal Data that is transferred out of the European Economic Area ("EEA"), Switzerland and the UK (together, "Europe") in connection with the use of Salesforce Services, and (iii) provides an overview of the assurances made by Salesforce to protect its Customers' data from inappropriate disclosure to law enforcement and intelligence agencies.

For the avoidance of doubt, this document should not be used to assess customer-specific use cases as the impact of processing Personal Data depends on the context of data usage by the Customers and the Customers' particular deployment of the Salesforce Services. Only our Customers are in a position to know and independently assess such customer-specific use cases. Customers are responsible for ensuring that their use of the Salesforce Services complies with their legal and contractual obligations.

Unless otherwise defined, capitalized terms in this document have the meaning as set out in the Salesforce Main Services Agreement ("MSA") and the Data Processing Addendum ("DPA").

PLEASE NOTE that transfer impact assessments are not required for transfers of Personal Data from Europe to US organizations certified under the EU-US Data Protection Framework. On July 10, 2023, the European Commission adopted an adequacy decision for the EU-US Data Protection Framework, concluding that the US ensures an adequate level of protection, compared to that of the EU, for personal data transferred from the EU to US organizations certified under the framework. Per the European Data Protection Board's 01/2020 Recommendations, explained in more detail below, where the European Commission has already declared the country, region or sector to which data is being transferred as adequate, organizations will not need to take any further steps, other than monitoring that the adequacy decision remains valid. You can find additional details about Salesforce's participation in our Notice of Certification under the framework.

UPDATED SEPTEMBER 2023

Table of Contents

1. Background: The Schrems II Ruling and EDPB Recommendations

Schrems II Ruling

On 16 July 2020, the Court of Justice of the European Union ("CJEU") issued its ruling in the "Schrems II" case[1]. In that ruling, the CJEU invalidated the EU-US Privacy Shield framework as a mechanism for transfers of personal data from the EU to the US. At the same time, the CJEU confirmed that the European Commission's standard contractual clauses ("SCCs") continue to be a valid legal data transfer mechanism for the transfer of personal data from Europe to non-adequate countries ("Third Countries"), while stipulating stricter requirements for the same. Specifically, it held that organizations conducting said transfers ("Data Exporters") are responsible for conducting diligence to help ensure compliance with European data protection laws, including assessing whether there is a level of protection for the personal data transferred that is essentially equivalent to that guaranteed by the GDPR, EU Charter of Fundamental Rights and the broader EU legal order. The CJEU also confirmed that, depending on the outcome of the above assessment, organizations might need to put in place supplementary measures to ensure there is an essentially equivalent level of protection. Accordingly, Data Exporters, relying on Article 46 GDPR transfer tools (e.g., SCCs or binding corporate rules), must carry out these assessments.

EDPB Recommendations

After the Schrems II decision, the European Data Protection Board issued non-legally binding recommendations ("EDPB Recommendations")[2] setting out a non-exhaustive list of protections organizations can take when transferring personal data from Europe to Third Countries to ensure an essentially equivalent level of protection for data transferred.

The EDPB Recommendations endorse the following six-step data transfer assessment ("EDPB Transfer Impact Assessment"):

Step 1: Identify International Data Transfers. Perform a mapping of international data transfers and assess whether the data transferred is adequate and limited to what is strictly necessary.

Step 2: Identify Data Transfer Mechanism(s). Verify the transfer tool(s) on which the transfer relies.

[1] Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems.

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Step 3: Assess the Laws or Practices of the Third Countries. These laws or practices may impinge on the effectiveness of the appropriate safeguards of the transfer tool, including using Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Step 4: Adopt Supplementary Measures. If the laws or practices of the Third Countries mean that the use of the transfer tool alone would not provide an essentially equivalent level of protection, identify the supplemental contractual, technical, or organizational measures that are necessary to bring the level of protection of the data transferred up to the European standard of essential equivalence.

Step 5: Adopt Necessary Procedural Steps. Take any formal procedural steps the adoption of any supplementary measure(s) may require.

Step 6: Re-evaluate, at appropriate intervals, the level of protection afforded to the data that the Data Exporter transfers to Third Countries, and monitor if there have been or there will be any developments that may affect it.

Standard Contractual Clauses

In June 2021 the European Commission issued new SCCs[3] ("2021 SCCs") which contain a requirement in Clause 14 to assess whether the laws and practices of the Third Countries to which personal data is being transferred could prevent the data importer from complying with the SCCs. When carrying out such an assessment, the parties declare that they have taken specific factors into consideration, such as the circumstances of the transfer, law and practices of the Third Country, and relevant contractual, technical or organizational safeguards put in place.

2. Description of Transfers

This section helps Customers perform step 1 of the EDPB Transfer Impact Assessment:

Step 1: Identify International Data Transfers.

Below, we describe the scenarios where personal data may be transferred from Europe to Third Countries with regards to the use of Salesforce Services.

[3] Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 available here.

A. Customer Support

Purpose and Details of the Transfer

Salesforce provides 24/7 Customer support using a "follow the sun" model. In order to resolve certain Customer support tickets, the Salesforce support team may require access to the Customer's Salesforce environment, which may include access to Personal Data submitted by Customers to the Salesforce Services. Unless specifically authorized by the Customer, Salesforce support staff do not have access to the Customer's Salesforce environment. Customer's Users may choose to provide the Salesforce support team with temporary access through temporary login credentials ("Grant Login Functionality"). Customers can specify the duration of such access and are able to revoke access at any time.

The frequency of any transfers of Personal Data for Customer support purposes depends on the number and type of support queries raised by the Customer and whether the Customer provides access through the Grant Login Functionality or not.

Locations from which Customer support is provided

The locations from which Customer support may be provided are set out in the Salesforce Infrastructure and Subprocessors Documentation.

Categories of Personal Data transferred

The categories of Personal Data that may be transferred for this purpose depend on the nature of the support case, the level of access provided by Customer, and the categories of Personal Data submitted to the Salesforce Services by the customer.

B. Technical Operations Support

Purpose and Details of the Transfer

To respond to technical or service problems, a dedicated team of Salesforce database administrators may, on occasion, require remote access to the database tables on which Customers' Personal Data is hosted following strict access and monitoring controls. More information on this process is available through the Salesforce Compliance Portal. The following operations may involve accessing the raw data without context (also see section 5 below) contained in the database:

- Management of servers, connections and networks
- Providing technical and networking service
- Maintaining operations
- Troubleshooting hardware issues
- Quality assurance testing

Locations from which Technical operations support is provided

The locations from which technical operations support may be provided are set out in the Salesforce Infrastructure and Sub-processors Documentation.

Categories of Personal Data transferred

The categories of Personal Data that may be transferred depend on the categories of Personal Data submitted to the Salesforce Services by Customer.

C. Storage of Personal Data Outside Europe

Purpose and details of the transfer

For most Salesforce Services, Salesforce offers Customers the ability to store their Customer Data in Europe. However, for some of the Salesforce Services and features, Customer Data may be stored or processed outside of Europe.

Locations outside of Europe where Personal Data may be stored

The locations outside of Europe where Personal Data may be stored are set out in the Salesforce Infrastructure & Sub-processor Documentation.

Categories of Personal Data transferred

The categories of Personal Data that may be transferred depend on the categories of Personal Data submitted to the Salesforce Services by the Customer.

D. User Information Replication

Purpose and details of the transfer

When Users log in to the Customer's Salesforce environment, login requests will be sent to the nearest data center for authentication. The authentication process redirects the User to the

appropriate data center for the duration of the active session. Salesforce may temporarily store identifying information about Users across its data storage locations outside of Europe for the purpose of facilitating the login process, even if all Personal Data is stored within Europe.

Alternatively, Customers can implement the MyDomain feature, which provides a different login routing mechanism that does not require the replication of Users' Personal Data to the other data storage locations. If MyDomain is enabled, Customers can contact the Salesforce support team to have the replication of User data deactivated.

Locations where User information may be temporarily stored

The locations where User information may be stored are set out in the Salesforce Infrastructure & Sub-processor Documentation for the relevant Salesforce Service.

Categories of Personal Data transferred

Personal Data shall only include the following information as it is provided by Customer in its provision of User accounts: first and last name, email address, username, phone number, and physical business address.

E. Content Delivery Networks

Purpose and details of the transfer

Content delivery networks ("CDNs") are utilized to optimize content delivery for certain Salesforce Services as listed in the Salesforce Infrastructure & Sub-processor Documentation. CDNs are commonly used systems of distributed services that expedite the transmission of content. Typically, a CDN is used to securely cache copies of content globally to better support end-users of the applicable Salesforce Services. Salesforce makes available the use of certain CDNs in conjunction with the Salesforce Services. In certain circumstances, Customers may also use their own CDN services in connection with the Salesforce Services or layer additional CDN functionality on top of the functionality made available by Salesforce.

More information on the various CDN services can be found in the Salesforce Infrastructure & Sub-processor Documentation.

Locations where Customer Data may be cached

More information on the locations where Customer Data may be cached (temporarily stored) can be found in the Salesforce Infrastructure & Sub-processor Documentation.

Categories of Personal Data transferred

The categories of Personal Data that may be transferred depend on the categories of Personal Data submitted to the CDN by the Customer.

3. Transfer Tools

This section helps Customers perform step 2 of the EDPB Transfer Impact Assessment:

Step 2: Identify data transfer mechanisms.

When transferring Personal Data to Third Countries, Salesforce uses two independent transfer mechanisms, both of which are incorporated into Salesforce's DPA:

- EU and UK Binding Corporate Rules for Processors ("BCRs") - company-specific, group-wide data protection policies approved by data protection authorities to facilitate transfers of Personal Data outside of Europe or the United Kingdom within the Salesforce group; and
- Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "2021 SCCs") - legal contracts entered into between contracting parties who are transferring Personal Data outside of jurisdiction to countries that have not been deemed adequate.

For further information, please see Salesforce's International Data Transfers FAQs, available here.

4. Potential Privacy Risks Under Local Laws and Relevant Practice

This section helps Customers perform step 3 of the EDPB Transfer Impact Assessment:

Step 3: Assess the laws or practices of the Third Countries.

This section describes possible privacy risks with regard to potential inappropriate disclosure to law enforcement and intelligence agencies associated with the data transfers described above. This section also briefly elaborates on Salesforce's practical experience in this regard, which is relevant for Customers when assessing the actual risks.

Transfers to the United States

The Schrems II ruling focused European attention on the breadth of law enforcement powers, particularly with respect to national security programs that permit US government agencies to engage in proactive surveillance. Salesforce recognizes that this has generated uncertainty about the impact of such US laws on EU data transfers. To address these issues, we have set out specific information about certain US laws considered by the CJEU ruling and their application to the Salesforce Services in this section. We also include information on the US Executive Order on Enhancing Safeguards for the US Signals Intelligence Activities, which introduces new binding safeguards to address the concerns raised by the CJEU in its Schrems II ruling. Crucially, these newly introduced binding safeguards have been deemed to meet the necessary EU guarantees by the European Commission as part of its adequacy decision on the EU-US Data Protection Framework.[4]

All of the safeguards that have been put in place by the US Government in the area of national security, including the redress mechanism described below, apply to all data transferred to the US, regardless of the transfer tool used. When assessing the effectiveness of the Article 46 GDPR transfer tool chosen, data exporters should be guided by the assessment conducted by the European Commission in its adequacy decision for the EU-US Data Privacy Framework, including the changes to US law that strengthen the privacy and civil liberties protections applicable to US signals intelligence activities, as a mitigating factor. The European Commission's adequacy decision greatly simplifies TIAs for transfers to the US based on SCCs and BCRs, as US law can now be considered to provide sufficient protection. Thus, organizations can confidently rely on these findings for the purposes of their TIAs and categorically conclude that no additional safeguards beyond the SCCs or BCRs are required. Nevertheless, Salesforce provides industry-leading contractual, technical, and organization frameworks and safeguards described herein.

Executive Order 12333 ("EO 12333")

EO 12333 authorizes and governs surveillance activities by US intelligence agencies. As the CJEU noted, the primary concern regarding EO 12333 is the US government's ability to collect personal data while it is in transit to the US by intercepting data travelling over transatlantic cables. Personal Data can effectively be protected from this type of interception through security measures such as encryption. Salesforce addresses this risk today by encrypting Personal Data and only transferring data that is subject to these strong protections. Please see section 5 below for more information about these measures.

[4] See paragraphs 119 to 204 of Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, available at Adequacy decision EU-US Data Privacy Framework_en.pdf (europa.eu).

It is important to note that EO 12333 does not grant the US government the ability to compel companies to provide assistance with the above activities. Moreover, Salesforce contractually commits to its Customers that it will not do so voluntarily. As a result, Salesforce does not and cannot be ordered to take any action to facilitate the type of bulk surveillance under EO 12333 that was considered problematic in the Schrems II ruling.

FISA Section 702

Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") sets forth processes and conditions for US intelligence agencies to lawfully collect information relating to non-US persons who are reasonably believed to be located outside the US if a significant purpose of such collection is to acquire foreign intelligence information and the source of the information is a US-based electronic communication service provider ("ECSPs").

FISA Section 702 authorizes "upstream" and "downstream" collection.

Upstream collection authorizes US authorities to collect communications as they travel over the internet backbone. Salesforce does not provide such backbone services, but only carries traffic involving our own Customers. As a result, Salesforce is not eligible to receive the type of orders principally addressed in, and deemed problematic by, the Schrems II ruling.

Downstream collection authorizes US authorities to collect targeted data directly from ECSPs based in the US. To the extent Salesforce may be compelled to respond to such a targeted request for Customer Data, we will carefully review the request to verify it is lawful and challenge the request in accordance with Salesforce's principles and contractual commitments on government access requests as further described in section 5 below.

More information on the surveillance program operated pursuant to FISA Section 702 can be found here.

US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act")

The CLOUD Act, enacted in 2018, clarifies existing legal frameworks and retains meaningful limitations on US law enforcement's ability to request data, for example: Companies must be subject to the jurisdiction of US law enforcement agencies. The CLOUD Act further confirms that the physical location of data is not the deciding factor but whether the recipient of a request has "possession, custody, or control" of the data. Requests are subject to the existing high standards and procedures for making such a request. Lastly, the CLOUD Act also established additional safeguards, including explicitly allowing companies to challenge disclosure requests that conflict with another country's laws.

To the extent Salesforce may be compelled to respond to such a law enforcement request for Customer Data, we will carefully review the request to verify it is lawful and challenge the request, in accordance with Salesforce's principles and contractual commitments on government access requests as further described in section 5 below.

Executive Order on Enhancing Safeguards for the US Signals Intelligence Activities ("EO 14086")

EO 14086 addresses key issues raised by the CJEU in the Schrems II ruling, provides binding safeguards that limit access to data collected by US surveillance activities, and enhances US oversight of surveillance intelligence.

In particular, EO 14086:

- Requires that surveillance activities be conducted only when necessary to advance a validated intelligence priority and only to the extent and in a manner that is proportionate to the authorized priority;
- Mandates handling requirements for personal information collected through surveillance activities and extends the responsibilities of legal, oversight, and compliance officials to ensure that appropriate actions are taken to remediate incidents of non-compliance;
- Calls for each element of the US Intelligence Community that engages in intelligence collection activities to update their policies and procedures to reflect the new privacy and civil liberties safeguards contained in the present EO; and
- Creates a two-tier mechanism, including a new Data Protection Review Court, for individuals from qualifying states and regional economic integration organizations (e.g., EEA) to obtain independent and binding review and redress.

On July 3, 2023, the US government fulfilled its commitments under EO 14086, as part of the EU-US Data Privacy Framework, to which President Biden and European Commission President von der Leyen agreed in March of 2022. More information on EO 14086 can be found here.

Relevant practice

The EDPB Recommendations also enable Customers to take into account Salesforce's practical experience "with relevant prior instances of requests for access received from public authorities" when performing their transfer impact assessment.

Salesforce's Transparency Report shows that it is rare for Salesforce to receive non-European government access requests for European Customers' data. Due to the nature of our business,

Salesforce generally does not process data that is of any interest to US or other non-European law enforcement or intelligence services. Generally, law enforcement finds it more efficient to approach Customers directly given that they are familiar with the specific configuration of their Salesforce environment and therefore know best where in the data model the relevant data is and what it is being used for.

For more information regarding Salesforce's commitment to transparency and how we deal with government access requests, please see section 5 below.

In addition, we would like to point our Customers to the white paper from the US Department of Commerce, Department of Justice, and Office of the Director of National Intelligence. The white paper outlines the limits and safeguards in the US relating to government access to data in response to the Schrems II ruling, notably that:

- Most US companies do not deal in data that is of any interest to US intelligence agencies and therefore do not pose a risk of the nature highlighted in Schrems II.
- Companies whose EU-US transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data.

In summary, Salesforce's relevant practice as demonstrated by the Transparency Report shows that the compelled disclosure scenarios that were flagged in the Schrems II ruling as potentially being high-risk with respect to the consumer service at issue in that case are in fact low risk when it comes to use of Salesforce Services.

Transfers to other countries

Salesforce contractually warrants that it has no reason to believe that the laws and practices applicable to the processing of Personal Data by Salesforce or its Sub-Processors prevent Salesforce from fulfilling its obligations under the DPA or otherwise pose any materially different privacy risks as to inappropriate disclosure of Personal Data to foreign government law enforcement and intelligence agencies.

5: Safeguards In Place to Ensure an Equivalent Level of Protection

This section helps Customers perform steps 4, 5, and 6 of the EDPB Transfer Impact Assessment:

Step 4: Adopt supplementary measures.

Step 5: Adopt necessary procedural steps.

Step 6: Re-evaluate.

This section summarizes the various contractual, technical, and organizational measures that Salesforce makes available to ensure that an equivalent level of protection exists for European Personal Data subject to cross-border transfers by Customers in connection with their use of the Salesforce Services.

In this section, we further explain why these measures ensure an equivalent level of protection and therefore allow for a lawful transfer of Personal Data outside Europe using the Salesforce Services.

Please see the Salesforce Security, Privacy and Architecture Documentation for each relevant Salesforce Service for a more comprehensive overview of the measures in place to ensure protection of Personal Data.

We encourage our Customers to regularly re-evaluate the level of protection afforded to Customer's data transferred to Third Countries.

Contractual safeguards

Salesforce Binding Corporate Rules

Salesforce has two sets of Binding Corporate Rules for Processors, one for EU transfers and another set for UK transfers.

EU BCRs: Salesforce's EU BCRs have been approved by all EU data protection supervisory authorities, including our lead regulator, the French Commission nationale de l'Informatique et des libertes ("CNIL"), and contain specific protections from government requests for access to EU personal data (Section 10). This includes obligations for Salesforce to report annually the government access requests it receives to the CNIL and to challenge overbroad government access requests that would lead to an unjustified disclosure of Personal Data. BCRs reflect the highest data protection standards in existence and remain the "gold standard" for transfer mechanisms.

UK BCRs: Salesforce's UK BCRs were approved by the UK data protection authority, the Information Commissioner's Office (ICO), in January 2023. Salesforce was one of the first six organizations in the UK to receive approval for its UK BCRs. The UK BCRs contain similar protections against overly broad government access requests as noted above in the EU BCRs.

Standard Contractual Clauses

Salesforce has made available to all Customers the 2021 SCCs, which contain extensive protections around compelled disclosure and international data transfers. The 2021 SCCs were specifically drafted by the European Commission and approved by all EU member states subsequent to the Schrems II ruling in order to provide appropriate safeguards to allow for a lawful international transfer of personal data. This includes a warranty from Salesforce that it has no reason to believe that local laws applicable to Salesforce would prevent it from offering an adequate level of protection of Personal Data.

Contractual Commitments

Salesforce has also extended extensive protections around compelled disclosure in respect of all Customer Data in its DPA (see section 8 "Government Access Requests") and these protections are offered to all Customers globally (i.e., including where Customer Data stays within Europe). Salesforce strongly believes that these contractual protections provide Customers as much legal certainty as possible in relation to compelled disclosure both within Europe and internationally.

As part of these contractual commitments:

- Salesforce will maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense, and public security.
- If Salesforce receives a legally binding request to access Personal Data from a Public Authority, it will (unless otherwise legally prohibited) promptly notify the relevant Customer, including a summary of the nature of the request.
- To the extent that Salesforce is prohibited by law from providing such notification to the relevant Customer, Salesforce shall seek to obtain a waiver of the prohibition to enable Salesforce to communicate as much information as possible, as soon as possible.
- Further, Salesforce commits to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful.
- Salesforce will pursue possibilities of appeal. When challenging a request, Salesforce commits to seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits.

- Salesforce will not disclose the Personal Data requested until required to do so under the applicable procedural rules.
- Salesforce also commits to provide the minimum amount of information permissible when responding to a request for disclosure based on a reasonable interpretation of the request.
- Salesforce will also promptly notify the Customer if it becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Salesforce in this respect, to the extent permitted by law.

Technical safeguards

Salesforce is committed to achieving and maintaining the trust of our Customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our Salesforce Services, including offering industry-leading technical measures to protect Personal Data against unauthorized access, as further described in this section.

An overview of the standard security controls applicable to the Salesforce Services is provided in the Salesforce Security, Privacy and Architecture Documentation. In addition, Salesforce offers a comprehensive set of security controls, as described below, which can help a Customer configure their Salesforce environment in line with a Customer's own security standards.

Encryption

A key technical supplementary measure described in the EDPB Recommendations is encryption, including the management of encryption keys. Salesforce offers enhanced encryption services that Customers can leverage to protect their Customer Data.

- Encryption in transit (default for all Salesforce Services)

  Salesforce Services use, or enable Customers to use, industry-standard encryption services to protect Customer Data and communications during transmissions between a Customer's network and the Salesforce Services. Additionally, all Customer Data is encrypted in transit between Salesforce data centres.

  Where appropriate, encryption in transit is also applicable between a Customer's existing application and the Salesforce Services if a Customer chooses to integrate its existing third party applications with the Salesforce Services through available application programming interface ("API") services.

- Encryption at rest and Bring Your Own Key ("BYOK") (optional add-on for the Salesforce Services)[5]

  The Salesforce Shield Platform Encryption solution encrypts selected data at rest when stored on our servers, in the database, in search index files, and the file system. To encrypt data at rest and preserve functionality, we built the encryption services natively into the Salesforce platform in line with industry-accepted encryption standards, such as the Advanced Encryption Standard (AES)

  Shield Platform Encryption allows Customers to manage the lifecycle of their own encryption keys while protecting those keys from unauthorized access by using hardware security modules ("HSM"). Key material is easily generated and controlled on demand using HSMs embedded in the key management service ("KMS") or supplied by the Customer using the BYOK service. The BYOK service allows Customers to generate and manage their key material outside of Salesforce and grant Shield Platform Encryption's key management systems access to these keys via an API service.

- Cache-Only Key Service (optional add-on for Customers that use Shield Platform Encryption)

  The Cache-Only Key Service addresses a unique need for non-persisted key material. Customers can create and store their key material outside of Salesforce. The encryption keys are fetched on demand from a key service that Customers control. Salesforce does not retain Customer's cache-only keys in any system of record or backups.

  For more information on Salesforce Shield Platform Encryption, BYOK and Cache-Only Key Service, please see here.

Polymorphic storage of data (default for all Salesforce Services)

Customer Data submitted to Salesforce Services is stored in a Salesforce database in a "polymorphic" manner. The data of thousands of customers may be stored in the same database table without context.

The data elements within the database are not useful or decipherable because they are without the context provided by the application and its logic. Therefore, it is not possible to identify a specific Customer.

The raw data elements in the database can only be deciphered when they are combined with the metadata of Customer's Salesforce environment. It is important to note that Salesforce database

[5] Shield Platform Encryption is available for most of the Salesforce Services. A list of Salesforce Services that currently do not support Shield Platform Encryption can be found here.

administrators with access to the database when providing technical operations support (see section 2B above) will never have access to Customer's Salesforce environment. And Salesforce support staff that has been granted temporary access to Customer's Salesforce environment when providing customer support (see section 2A above) will never have access to the database.

Organizational safeguards

Salesforce has a number of organizational safeguards in place to protect personal data processed in the context of the Salesforce Services to ensure that the contractual commitments noted above are complied with in practice.

Transparency

At Salesforce, we believe that trust starts with transparency and we want to be transparent about our commitments to protecting our Customers' data in our Salesforce Services.

This commitment is highlighted in our Transparency Reports, which details the types and numbers of the requests we receive from law enforcement and other government agencies, as well as how we respond to them. It also shows that it is rare for Salesforce to receive non-EU government requests for Customer Personal Data.

If Salesforce is compelled to respond to a government request for Customer Data, we will carefully review the request to verify that it is lawful, following the principles in this document and the contractual commitments that we outlined above.

Internal Policies

Salesforce has internal policies, including globally applicable standards and processes, which govern Salesforce's approach to responding to requests to access Personal Data from governments. A dedicated and specifically trained team of Salesforce lawyers will be analyzing, responding to, and documenting these types of requests to ensure that we are fulfilling our contractual commitments and legal obligations.

6. Salesforce Determines Equivalent Protection of Personal Data

As outlined above, when assessing potential data protection risks in relation to compelled disclosure and international data transfers post Schrems II, the GDPR requires that data importers and data exporters should take into account the specific circumstances of the transfer and any safeguards put in place (including relevant contractual, technical, and organizational measures applying to the Personal Data). In other words, a holistic approach is required in which the entire array of contractual, technical, and organizational security measures offered by Salesforce and

those that can be implemented by Customers need to be considered so that an appropriate risk assessment can be made. The GDPR does not require that organizations eliminate all risk, which would be impossible, but to take appropriate measures to mitigate risks.

Taking into account the information set out in this document, Customers can use Salesforce Services to transfer their data outside of Europe in compliance with European law by relying on the industry-leading contractual, technical, and organizational frameworks described in this document.