DMP: Fact Sheet and DPIA

This document provides more information about the privacy and security of the Salesforce DMP which can help our customers to assess our security and privacy program, including by completing privacy impact assessments. It does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation. More information about privacy impact assessments can be found here.

GDPR and the DMP

At Salesforce, trust is our #1 value, and nothing is more important than the success of our customers and the protection of their data. Salesforce enables our customers to build trusted relationships, putting their customers at the center of everything they do, including protecting individual privacy through GDPR compliance.

The General Data Protection Regulation ("**GDPR**") is a European privacy law effective on May 25, 2018. The GDPR expands the privacy rights of EU individuals and places new obligations on all organizations that market, track, or handle EU personal data. For more information about the GDPR, please refer to our Salesforce GDPR website, specifically our GDPR Key Facts paper, which defines a number of the terms used in this document.

Salesforce welcomes this law as an important step forward in streamlining data protection requirements across the European Union and as an opportunity for Salesforce to deepen our commitment to data protection. Similar to existing privacy laws, compliance with the GDPR requires a partnership between Salesforce and our customers in their use of our services. We're committed to complying with the GDPR in providing services to our customers as a processor. And we're committed to ensuring that our customers can continue to use our services while complying with GDPR. As part of our commitment to our customers, we've published this document to describe the features customers can use when responding to common GDPR requests using the Salesforce DMP[1], and to assist our customers in completing their data protection impact assessment for the Salesforce DMP. Capitalized terms not defined herein have the meaning set forth in Salesforce's Master Subscription Agreement and/or Data Processing Addendum.

[1] This document covers the services branded as Salesforce DMP (formerly branded as Krux), Salesforce Data Studio, or services sold under a Krux Order Form (the "Salesforce DMP") This document does not apply to other Salesforce services that may be associated with or integrate with the Salesforce DMP, such as Marketing Cloud Services.

Security

The GDPR requires organizations to use appropriate technical and organizational security measures to protect personal data against unauthorized processing and accidental disclosure, access, loss, destruction, or alteration. Salesforce has robust security and privacy programs in place that meet the highest standards in the industry. They enable us to comply with a variety of data protection laws and regulations applicable to Salesforce.

Architecture

The Salesforce DMP is operated in a multitenant architecture that is designed to segregate and restrict customer data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

Security Controls

The Salesforce Services include a variety of security controls, policies and procedures, as further described in our Trust and Compliance Documentation. Salesforce, or an authorized independent third party will monitor the Salesforce DMP for unauthorized intrusions using network-based intrusion detection mechanisms. The Salesforce DMP uses, or enables customers to use, industry-accepted encryption products to protect customer data, which is encrypted in transit when uploaded to or downloaded from the Salesforce DMP, or Salesforce DMP-created applications using Transport Layer Security 1.2 (TLS). TLS is active on all accounts by default. Production data centers used to provide the Salesforce DMP have access control systems. These systems permit only authorized personnel to have access to secured areas.

Certifications

Salesforce's information security control environment applicable to the Salesforce DMP has undergone an independent evaluation in the form of the SOC 2, Type II audit. Additionally, the Salesforce DMP regularly undergoes security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis. Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Data Subject Rights

The GDPR grants data subjects a number of rights in respect of how organizations handle their data. These rights require companies to have systems in place to respond to and effectively address data subjects' requests. For example, if an individual submits a request to have their personal data deleted and the relevant circumstances apply, companies must be equipped to find the relevant personal data linked to that individual and delete it. The Salesforce DMP enables customers to process these requests by using the following tools within the products.

Basis of Data Processing and Right to Object: *In order to process personal data, organizations must have a lawful basis to process the data. Under the GDPR, there are six legal bases which organisations can rely on to lawfully process personal data. One basis for processing is with the consent of the data subject (the five other bases are (i) legitimate interest, (ii) contractual necessity, (iii) compliance with legal obligations, (iv) vital interest and (v) public interest). It is up to each Salesforce customer to determine which legal basis is most appropriate for their processing operations, and if they choose to rely on consent, obtain the appropriate consents from their data subjects. Consent under the GDPR must be freely given, specific, fully informed and an unambiguous indication of the data subject's wishes by clear affirmative action. Data subjects can in certain cases object at any time to the processing of their personal data, in particular if the processing is for direct marketing purposes.*

- The Salesforce DMP provides tools to customers to assist them in implementing consent flags to capture an individual's consent, where required. For more information about consent flags, please see the Concepts and Glossary of Terms.
- There are five methods available to pass consent to the Salesforce DMP: API, JavaScript Consent Tag, SDK, file upload, and Salesforce DMP user interface (UI); we recommend using the API, JavaScript Consent Tag, and SDK methods as described in the DMP Implementation Best Practices for GDPR.

For more details about consent management and the Salesforce DMP, please see the Consent Management Documentation.

Data Access and Data Portability: *Data subjects have the right to confirm with a data controller whether the organization is processing their personal data. If it is, the controller must provide the data subject with information about such processing, including the specific data processed, the purposes of the processing, and the other parties with whom such data has been shared. In certain cases, data subjects have the right to ask a controller to provide their personal data in a structured, commonly used, and machine-readable format so that they can transmit their own personal data to another company.*

Both the rights of data access and data portability require the extraction of personal data through a data feed. There are five available methods within the DMP to request data feeds: API, JavaScript Consent Tag, SDK, file upload, and Salesforce DMP UI. Salesforce DMP will deliver the data feeds within 14 days of the request. Access and portability data feeds will be segregated by user ID and data source, and deposited at the following location: s3://krux-partners/client-{org_name}/portability/{date}/{data_source}/{IDValue}/

For more details about data portability and the Salesforce DMP, please see the Data Portability Management Documentation.

Data Rectification: *Data subjects can request that a controller correct or complete personal data if the data is inaccurate or incomplete.*

- Customers can correct personal data about an individual by uploading a new version of that subset of Customer Data, which will update the information about the individual.
- To update or correct Content (data provided by or purchased from second and third parties, including via Data Studio) customer should contact the provider or owner regarding any correction.

Right to Erasure: *Also known as "the right to be forgotten," this right empowers data subjects to request that a data controller delete or remove their personal data in situations such as the following: when the data is no longer needed for the original purpose, when the data subject withdraws consent, or when the data subject objects to the processing and the controller has no overriding legitimate interest in the processing. A data subject can request personal data be deleted from the controller through the lines of communication that the controller sets up to accept such requests.*

Customers may request data deletion by providing a single user ID or multiple user IDs via API, SDK, JavaScript Consent Tag, or file, or by selecting the user ID type and populating the IDs in the Salesforce DMP UI. Once requested, Salesforce deletes all Customer Data from the Salesforce DMP that is tied to the submitted identifier(s). This happens within 90 days of the initial request. Deleted data includes, but is not limited to:

Segments
Ad Impressions
Events
Transactions
User's Page Views
User Attributes
Heartbeats

For more details about data portability and the Salesforce DMP, please see the Data Deletion Management Documentation.

Restriction of Processing: *Data subjects can request that a controller block or suppress the processing of their personal data. For example, the controller can mark or use technological means to ensure that such data will not be further processed by any party. This may be relevant if a customer temporarily restricts processing operations until their records are updated or in the case of a legal hold being placed on certain customer records.*

The Salesforce DMP provides functionality by which customers may restrict the processing of Customer Data related to an individual, for example, by disabling the collection or analysis of such Customer Data.

In addition to the information contained in this section, we recommend reading the DMP Implementation Best Practices for GDPR.

Answers to Common Data Protection Impact Assessment Questions about the DMP

I. SCOPE

This document is designed to help customers by providing information they can use to complete their own privacy impact assessments or data protection impact assessments about their use of the Salesforce DMP.

II. OVERVIEW OF PERSONAL INFORMATION

Provide a general description of the Service.

Salesforce provides its customers with software-as-a-service solutions, including the following services covered in this document:
Salesforce DMP is a data management platform that manages data, identifies end users, and centralizes user-level data for advertising and content personalization.
Salesforce Data Studio is a platform that connects buyers and sellers of second party data.

Describe the Personal Data that will be used, stored, collected, disclosed or otherwise Processed on the Service.

Salesforce DMP customers choose what data to submit to, and collect with, the Salesforce DMP. Typical personal data processed on behalf of customers would include data related to

consumers' internet browsing activities (e.g., websites visited or advertisements viewed), which data is then tied to pseudonymous device identifiers such as cookies and mobile identifiers. Customers are prohibited from submitting personal data (such as names, email addresses, or user names) to the Salesforce DMP other than pseudonymous personal data and IP address. In addition, as the Salesforce DMP adheres to the Network Advertising Initiative (NAI) Code of Conduct (https://www.networkadvertising.org/code-enforcement/code), the Salesforce DMP may not be used: (i) to associate pseudonymous non-personal identifiers with other personal data in violation of the NAI Code of Conduct; and/or (ii) to use cookies, web beacons, or other tracking mechanisms to collect or store personal data in violation of the NAI Code of Conduct.

Does the Personal Data include "special categories of Personal Data" (as defined under GDPR) or Personal Data related to criminal convictions or offences?

No. Customers are prohibited from submitting personal data to the Salesforce DMP other than pseudonymous personal data and IP address. Furthermore, sensitive data that is regulated by data protection laws or regulations may not be submitted to the Salesforce DMP, including but not limited to, government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); data pertaining to an individual's health or medical condition, sexual orientation, religion, or status such as a person under the age of 18 years of age; and data defined as Sensitive Data under the NAI Code of Conduct or Digital Advertising Alliance (DAA) Self-Regulatory Principles.

Does the Personal Data include financial account numbers, government identification numbers, or health information?

No. Customers are prohibited from submitting personal data to the Salesforce DMP other than pseudonymous personal data and IP address. Furthermore, sensitive data that is regulated by data protection laws or regulations may not be submitted to the Salesforce DMP, including but not limited to, government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); data pertaining to an individual's health or medical condition, sexual orientation, religion, or status such as a person under the age of 18 years of age; and data defined as Sensitive Data under the NAI Code of Conduct or Digital Advertising Alliance (DAA) Self-Regulatory Principles.

Where are the Data Subjects located?

This depends on how the customer uses the Salesforce DMP. For example, the locations of consumers will depend on: (i) what information the customer submits to the Salesforce DMP; (ii) where the customer's authorized Users of the Salesforce DMP services are located; and (iii) the countries from which consumers access any Salesforce-hosted application or website.

What is the general purpose for Processing the Personal Data?

Customers using the Salesforce DMP are generally agencies and advertisers that use the Salesforce DMP to reach consumers with personalized and relevant content.The Salesforce customer, as the data controller, should determine its specific purpose for processing Personal Data on the Salesforce DMP. Salesforce processes Personal Data to offer the Salesforce DMP, under the terms agreed to in the contract.

Could the Processing of the Personal Data have an impact on key aspects of an individual's life?

How Salesforce's Processing of Personal Data affects key aspects of an individual's life will depend upon the Salesforce customer's use case.

Are the Data Subjects made aware of the details of the Processing of their Personal Data?

Salesforce does not directly communicate with its customers' consumers, and consumers' awareness of the data processing is the Salesforce customer's responsibility. To the extent consumers are interested in Salesforce's specific practices, Salesforce's Privacy Statement and other privacy-related documentation are available here.

III. ACCESS TO PERSONAL DATA

How is Personal Data managed in the Service?

Salesforce's user interface allows customers to manage their own Customer Data, including Personal Data, on the Salesforce DMP. To the extent customers need Salesforce's assistance in managing Personal Data, Salesforce has committed to provide assistance as described in its Data Processing Addendum. The current, GDPR-ready version of Salesforce's Data Processing Addendum is available here.

How is access to the Service managed?

Customers can assign different levels of access to their Users. The Salesforce DMP also allows the customers to assign access permissions based on the User's role. Salesforce's customer contracts restrict access by Salesforce's personnel, who may access Personal Data only to provide the services, to prevent or address technical or service problems, if compelled by law, or with the Salesforce customer's written permission.

Who will manage security of the Salesforce DMP?

Salesforce has policies and procedures in place to protect the security of the Salesforce DMP. The security policies, procedures, and controls Salesforce makes available to customers are described in the Security, Privacy and Architecture documentation available here. Salesforce customers share responsibility for managing security. The Salesforce DMP include a variety of security controls that a Salesforce customer can configure; each customer is responsible for

configuring those security controls and for managing other aspects of processing under its control such as the security of the customer's Users' computers, and controlling access to its instances of the Salesforce DMP.

Who is responsible for assuring proper use of the Personal Data?

Customers are responsible for using the Salesforce DMP appropriately, including their processing of Customer Data on the Salesforce DMP. Salesforce is responsible for providing the Salesforce DMP appropriately under its contract with its customers. Under that contract, Salesforce commits to using Personal Data only to provide the Salesforce DMP, to prevent or address service or technical problems, as compelled by law, or as the customer expressly permits in writing.

How can requests from individual Data Subjects to access or correct their Personal Data be handled on the Salesforce DMP?

The Salesforce DMP allows customers to manage the Personal Data they maintain in the Salesforce DMP, including in response to Data Subject requests. More detail about how to do so can be found in the DMP Implementation Best Practices for GDPR Documentation and the beginning of this paper. To the extent a customer needs Salesforce's assistance to respond to a Data Subject, Salesforce will provide assistance as described in Section 3 of its Data Processing Addendum, available here.

Can Salesforce personnel access Personal Data in the Salesforce DMP? If so, where are those personnel located and for what purpose do they need access?

Salesforce agrees by contract that its personnel may access Personal Data only to provide the Salesforce DMP, to prevent or address technical or service problems, if compelled by law, or with the Salesforce DMP customer's written permission. The locations of Salesforce's Affiliates that employ personnel who may access Personal Data for these purposes is available in the Infrastructure & Sub-processors Documentation, available here.

IV. INFORMATION SYSTEM DESIGN

Where will Personal Data be stored?

Salesforce's storage locations for Personal Data are described in the Infrastructure and Sub-processors documentation available here.

Will the Personal Data be stored in the European Union?

Under the GDPR, there is no requirement for personal data to be stored in the EU. As outlined in the preceding question, the Salesforce DMP's storage locations are described in the Infrastructure and Sub-processors documentation, and in some cases a customer may choose to have its own data servers located in the European Union. In addition, Salesforce DMP offers two mechanisms to legally transfer personal data outside of the EU: the EU-US and Swiss-US Privacy Shield certification, and the Standard Contractual Clauses. For more information about these transfer mechanisms please review the Salesforce Privacy Statement.

Describe the Salesforce DMP's information flow for Personal Data.

Salesforce DMP provides a cloud-based product, and customers can allow their Users to access the Salesforce DMP from virtually anywhere with an Internet connection. For these reasons, personal data may flow to or from Salesforce from global locations, depending on where the customer and its Users are located.

In terms of data flows within the Salesforce DMP:

- Personal Data about a Salesforce customer's Users: Customers enter Personal Data about their Users when they provision the Users' accounts. Personal Data may also be collected when Users perform activities on the Salesforce DMP—for example, when their actions generate records of their activities. In either case, the information flows from the location of the person entering the data to the Salesforce DMP's storage facilities.

- Personal Data about a Salesforce customer's consumers: At customer's direction, Salesforce DMP collects information about customer's app users, website visitors, and online advertising viewers. In this case, the information flows from the consumer's online location to the Salesforce DMP's processing and storage facilities as described in the Infrastructure and Sub-processors documentation.

- Personal Data accessed by Salesforce personnel: If Salesforce personnel access Personal Data—for example, if a customer requests that Salesforce access its data during a customer support inquiry—then the data will be visible to the Salesforce individual accessing the data. The locations of Salesforce and its sub-processors are described in the Infrastructure and Sub-processors documentation available here.

How are transfers across national borders accounted for? If a transfer takes place, what is the purpose of this transfer?

Salesforce's Data Processing Addendum, available here, offers multiple transfer mechanisms for the Salesforce DMP Services and includes an "order of precedence" clause. Specifically, Salesforce offers both EU-US and Swiss-US Privacy Shield certification and the Standard Contractual Clauses for the Salesforce DMP Services.

How (and with whom) will Personal Data be shared in the Salesforce DMP?

Personal Data is shared by a customer with Salesforce and, if applicable, its sub-processors, as described in the Infrastructure and Sub-processors Documentation available here. Access by Salesforce and its sub-processors is subject to the protections in the Data Processing Addendum available here, and Salesforce maintains safeguards to prevent access except (a) to provide the Salesforce DMP Services and to prevent or address service or technical problems, (b) as compelled by law, and (c) as the customer expressly permits in writing.

What contracts are in place to protect Personal Data submitted to the Service?

Protections for Personal Data are described in the Salesforce customer's contract with Salesforce. Contractual documents containing protections for Personal Data include (1) a Master Subscription Agreement (MSA) between Salesforce and the customer; (2) Salesforce's Data Processing Addendum, which can be added to the contract (if not already included) by following the instructions here; (3) and the Trust and Compliance Documentation, available here.

V. SECURITY AND DATA INTEGRITY

What technical security and physical security measures are in place to protect Personal Data from unauthorized access or disclosure?

Salesforce's policies and procedures to protect the security of Personal Data, and configurable security controls available to the Salesforce customer, are described in the Security, Privacy and Architecture documentation available here.

How are breach notifications addressed?

Salesforce has comprehensive procedures in place to notify customers in the event of a data breach of its systems as managed by its Computer Security Incident Response team (CSIRT). Salesforce commits contractually in its GDPR-ready Data Processing Addendum to notifying customers "without undue delay" which is the standard of notification required for processors under the GDPR. Salesforce has a formal Incident Management Process that guides the Salesforce Computer Security Incident Response team (CSIRT) in investigation, management, communication, and resolution activities.

Salesforce will promptly notify the customer in the event of any security breach of the Salesforce DMP resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce Support, email to the customer's administrator and Security Contact (if submitted by customer), and public posting on

trust.salesforce.com. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system.

Can Personal Data be masked?

Yes. The Salesforce DMP uses, or enable customers to use, industry-accepted encryption products to protect customer Data, which is encrypted in transit when uploaded to or downloaded from Salesforce DMP-created applications using Transport Layer Security 1.2 (TLS). TLS is active on all accounts by default.

Is security on the Salesforce DMP audited?

Yes. The Salesforce Services are subject to various audits and certifications, which are described in the Security, Privacy, and Architecture documentation, available here.

VI. RETENTION/DISPOSAL OF INFORMATION

How long is Personal Data retained in the Salesforce DMP?

Customers choose how long to retain Customer Data, including Personal Data, on the Service. Unless otherwise specified in the Trust and Compliance Documentation, Salesforce does not delete Customer Data, including Personal Data, during a subscription term, unless the customer instructs Salesforce to do so. After a customer's contract with Salesforce terminates, Salesforce deletes Personal Data in the manner described in the Security, Privacy and Architecture documentation, available here.

How is Personal Data disposed of when it is no longer needed?

Upon request by the customer, or after termination of a customer's contract, Salesforce deletes the customer's Personal Data in the manner described in the Security, Privacy and Architecture documentation, available here.

How are requests from Data Subjects to have their Personal Data deleted managed?

As described in Salesforce's Data Processing Addendum, available here, Salesforce shall notify a customer if it receives a request to exercise rights related to the processing of Personal Data on the services for which that customer is the Data Controller. The Services provide functionality to enable to the customer to respond to that request, but Salesforce's Data Processing Addendum also commits to provide reasonable assistance if needed.

VII. MISCELLANEOUS

Has Salesforce appointed a Data Protection Officer?

Salesforce has appointed Data Protection Officers or other points of contact under the requirements of current laws, and will appoint a Data Protection Officer under GDPR by May 25, 2018. Please reach out to privacy@salesforce.com to contact the Data Protection Officer.

Does Salesforce have a Privacy Policy?

Yes, Salesforce's privacy statements are available here.

Please provide an overview of how Salesforce incorporates the principles of "privacy by design" into its product development.

Salesforce works to incorporate privacy and data protection concepts from the inception of each new service or feature it offers. Product managers and engineers who design our products are trained at least annually on data protection. In addition, each Salesforce service is supported by at least one product attorney knowledgeable about data protection generally, and the GDPR in particular, and who reviews and advises on the product's functionality. And each of those attorneys is supported by a privacy attorney who specializes in data protection full-time. The product release cycle also contains multiple checks where additional people can provide comments on the service or features' protection of Personal Data. Finally, when a service or feature is released, it is described in product documentation and release notes so that customers can perform their own evaluations. Salesforce regularly considers input from its customers when designing and refining product functionality.

Please provide details of how Salesforce is addressing its accountability and governance obligations under the GDPR.

Salesforce commits to meeting its accountability and governance obligations under the GDPR and will take all appropriate related measures. These measures include implementing appropriate technical and organizational security measures (more details available in the Trust and Compliance documentation), undertaking privacy impact assessments (where appropriate) and maintaining records of processing, among others. Salesforce will also appoint a data protection officer as is required under the GDPR.

Are Salesforce employees bound by confidentiality obligations?

Yes, Salesforce commits in its GDPR-ready data processing addendum to ensure that personnel have been appropriately trained, are reliable and enter into confidentiality agreements. Employees also regularly undergo data protection training, such as the European Union Privacy Law Basics Trailhead.