Callidus Software Inc.
EU-U.S. Privacy Shield Notice

Effective as of December 7, 2016

Callidus Software Inc., doing business as CallidusCloud, together with its affiliates, which includes subsidiaries and entities that Callidus Software Inc. operates (collectively, "CallidusCloud," "we," or "us") complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding all Data About Customers (as defined in the CallidusCloud Privacy Policy) it received from the European Union in reliance on the EU-U.S. Privacy Shield. CallidusCloud has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in the Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit www.privacyshield.gov/.

"Personal data" and "personal information", as used herein, means personal data regarding Data About Customers from Individuals within the scope of the Directive 95/46/EC (other than human resources data) that is received by CallidusCloud and that is transferred from the European Union to the United States. For such data received from the European Union in reliance on the EU-U.S. Privacy Shield, the following requirements apply:

1. Information Collected and Use of Collected Information

We collect and use personal data as described in the CallidusCloud Privacy Policy (the "Policy"), which may be found at www.calliduscloud.com/privacy-policy/.

2. Right to Access

Individuals have rights to access personal data about them, and to limit use and disclosure of their personal data. The right to access includes the ability to correct, amend, or delete that personal data where it is inaccurate, or has been processed in violation of the Privacy Shield Principles, except where the burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated. Access rights according to the Privacy Shield Principles may also be restricted in some other cases, e.g. when a disclosure is likely to interfere with the safeguarding of important countervailing public interests. If you have any issues, questions or requests relating to Right to Access, please contact us at legal-privacy@calliduscloud.com.

3. Choice and Means for Limiting the Use of Your Personal Data

CallidusCloud will provide you with the possibility to opt out in case CallidusCloud wants to (i) disclose your Personal Data to a third party that is not acting as an agent on behalf of CallidusCloud, or (ii) use it for a purpose materially different from the purpose for which it was originally collected or subsequently authorized by you. In these cases, you can opt out by sending an e-mail to: info@calliduscloud.com.

For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), we will obtain your affirmative express consent (opt in) if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for

which it was originally collected or subsequently authorized by you through the exercise of opt-in choice. CallidusCloud is not required to obtain affirmative express consent (opt in) with respect to sensitive information where the processing is (a) in the vital interests of the data subject or another person; (b) necessary for the establishment of legal claims or defenses; (c) required to provide medical care or diagnosis; (d) necessary to carry out CallidusCloud's obligations in the field of employment law; or (e) related to information that is manifestly made public by the individual. CallidusCloud will treat as sensitive any Personal Information received from a third party where the third party identifies and treats it as sensitive.

Additionally, you may manage your receipt of marketing and non-transactional communications by clicking on the "unsubscribe" link located on the bottom of CallidusCloud's marketing emails or you may send a request to info@calliduscloud.com.

4. Third Parties Who May Receive Personal Data (Onward Transfers)

CallidusCloud uses a limited number of third party service providers to assist us in providing our services to our customers. These third-party service providers may access, process, or store personal data in the course of providing their services. In transferring such information to a third party, CallidusCloud will obtain assurances from such third party that it subscribes to the Privacy Shield Principles or otherwise safeguards Individuals' personal data consistently with the same level of privacy protection as is required by the Privacy Shield Principles. In the context of an onward transfer, CallidusCloud has responsibility for the processing of personal data it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. CallidusCloud shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless CallidusCloud proves that it is not responsible for the event giving rise to the damage.

5. Security

CallidusCloud will take reasonable precautions to protect personal data in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

6. Data Integrity

CallidusCloud will use personal data only in ways that are relevant for the purposes for which it was collected or authorized by the relevant Individual.

7. Enforcement

To ensure compliance with the Privacy Shield Principles, CallidusCloud will conduct an annual independent audit of its privacy practices, which shall include confirming: (a) the Policy, and notices regarding any changes to the Policy, are posted in a conspicuous place on CallidusCloud's website; (b) the Policy is accurate, comprehensive and conforms to the Privacy Shield Principles; (c) its annual renewal of EU-U.S. Privacy Shield self-certification with the US Department of Commerce; (d) CallidusCloud's inclusion of its name on the US Department of Commerce's EU-U.S. Privacy Shield list of compliant companies (www.privacyshield.gov/list); and (e) that appropriate employee training and internal procedures exist for periodic reviews of CallidusCloud's compliance with the Policy.

In addition, CallidusCloud commits to resolve complaints about privacy and the collection or use of personal data. Individuals with inquiries or complaints should first contact CallidusCloud, 4140 Dublin Blvd., Suite 400, Dublin, CA 94568, Attn: Chief Privacy Officer.

CallidusCloud has further committed to refer unresolved Privacy Shield complaints to Judicial Arbitration and Mediation Services (JAMS), an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgement of your complaint from us, or if we have not addressed your complaints to your satisfaction, please contact or visit www.jamsadr.com/eu-us-privacy-shield for more information or to file a complaint. The services of JAMS are provided at no cost to you.

8. FTC Jurisdiction

The Federal Trade Commission (FTC) has investigatory and enforcement power over CallidusCloud and its compliance with the Privacy Shield. The FTC also has jurisdiction to hear any claims of unfair or deceptive practices or violations of laws or regulations governing privacy. Under certain limited conditions, Individuals may be able to invoke binding arbitration for complaints regarding Privacy Shield compliance not resolved by any of the other Privacy Shield mechanisms.

You must take following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with CallidusCloud and afford us an opportunity to resolve the issue within 45 days of receiving your complaint; (2) make use of the independent dispute resolution mechanism, which is at no cost to you; and (3) raise the issue through your Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue, at no cost to for you. This arbitration option may not be invoked if your same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which you were a party; or (3) was previously settled by the parties. Please check https://www.privacyshield.gov/article?id=C-Pre-Arbitration-Requirements for further information.

9. Compelled Disclosure

CallidusCloud may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

This Policy was last modified on December 7, 2016