Privacy and Security

Frequently Asked Questions

CONFIDENTIALITY

DISCLAIMER

TABLE OF CONTENTS

INTRODUCTION

As our Customers operate globally, including in the United States and the European Union, we appreciate the importance providing information needed by Customers to evaluate whether our products and Services align with requirements of the regulatory landscapes in which they operate, including the EU General Data Protection Regulation 2016/679 (the "**GDPR**").

Following the July 2020 decision by the European Court of Justice ("**CJEU**") in the "Schrems II" case, subsequent European Data Protection Board recommendations ("EDPB Recommendations"), and the standard contractual clauses issued by the European Commission in June 2021 ("2021 Clauses") updating the prior version ("**2010 Clauses**"), we also recognize that you – our Customers – may have additional questions.

We are available to assist Customers in their analysis of Zuora's processes and procedures considering the Schrems II decision and 2021 Clauses. The following pages contain answers to frequently asked questions about Zuora and its Services, including (1) steps we have taken to further establish technical and organizational safeguards ensuring a level of protection that is provided within the European Union; (2) our use of standard contractual clauses when transferring personal data of European data subjects to a third country; (3) our efforts to update our data protection/processing agreements with our vendors who may access our Customer's personal data; and (4) information about our process for handling public authority requests.

Please do not substitute this information for legal advice (which Zuora cannot provide). We strongly encourage each Customer to perform its own due diligence when assessing its use of the Services in light of their own obligations under applicable law. However, this information is offered to brief you and your counsel on important considerations regarding our Services and the data protection efforts we have instituted at Zuora.

For additional information, please contact Zuora's Privacy Team at dpa@zuora.com.

GENERAL DESCRIPTION OF ZUORA SERVICES

Zuora provides a white-labeled subscription management platform along with related tools that are embedded in the respective Customer's environment (collectively, the "**Services**"). The Services facilitate Customer's ability to recognize revenue, simplify payment processes, increase first-time payment success, and streamline their users' experience when making payments.

For more information about our Services, please see https://www.zuora.com/products/ or speak with your dedicated account representative.

QUESTIONS ABOUT ZUORA'S SERVICES

What is Zuora's role under privacy law? What categories of personal data does Zuora handle for Customers?

Zuora acts as a processor and Service provider with respect to personal data submitted by Customers to the Services. Typically, Customers act as the controller for such personal data (or a processor on behalf of a controller). This means that each Customer uniquely determines what personal data is submitted to, and processed by, our Services. Typically, this data includes name, contact information, address, subscription-specific details and payment information. Customers are responsible for ensuring that submission of any special categories of personal data, where permitted, complies with applicable laws and the contractual terms in place with Zuora.

Zuora only processes personal data in accordance with our Customer's documented instructions. This is set out in Zuora's data protection and master subscription agreements.

Are data subjects made aware of the details of the processing of their personal data?

It is the Customer's responsibility to inform data subjects of its processing of their personal data using the Services. Zuora provides self-service tools that enable Customers to interact with data subjects and manage data within their tenant.

Zuora's global support team is available to assist any Customer who requires assistance with using these tools.

How does Zuora handle requests made by data subjects?

Zuora does not receive requests from Customer's end users. However, should such a request be received, Zuora will promptly suggest that the data subject contact the Customer directly. If a Customer does not wish Zuora to direct the requestor to the Customer, Zuora will notify the Customer of the request so that the Customer can decide if and how to respond.

Unless contrary to applicable law, Zuora will not further respond to any data subject request without the Customer's direction. This process is set out in Zuora's data protection and master subscription agreements.

Does Zuora use subprocessors when providing its Services?

Yes. Zuora uses subprocessors to host and maintain the effectiveness and efficiency of its Services. Its subprocessors include affiliates of Zuora as well as third party entities. Zuora updates its lists using normal communication channels to which we encourage each Customer to subscribe. A further process may be set out in Zuora's data protection and master subscription agreements.

Has Zuora updated its data processing agreements with its subprocessors?

Yes. Zuora entered into updated data processing agreements with all of its subprocessors and its affiliates to more clearly define roles and responsibilities, added supplementary measures and safeguard requirements and executed 2021 Clauses with each.

How does Zuora address cross-border data transfer restrictions?

Zuora updated its data processing agreement to more clearly define the roles and responsibilities of itself and its Customers. Its data processing agreement incorporate by reference applicable modules of the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and, where applicable, standard data protection terms adopted in the United Kingdom.

Will Zuora notify Customers in the event of a security breach?

Yes. Zuora commits to notifying its Customers without undue delay after determining that an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed by Zuora or its subprocessors has occurred.

Zuora has a dedicated security incident team along with procedures to manage incidents and breaches within our Services ("**Security Incident Response Procedures**"). Zuora's leadership regularly reviews the Security Incident Response Procedures to ensure that they are up to date.

What happens to Customer's data after termination or expiration of its master subscription agreement with Zuora?

After termination or expiration of the master subscription agreement, Zuora will delete Customer's data in accordance with its policies and procedures and within the timeframes specified in either the master subscription or data protection agreement.

Where is Customer's personal data stored? Does Zuora access Customer's personal data from outside of the European Union?

Zuora utilizes a third-party cloud provider, Amazon Web Services, to host both its US and EU-based data centers. Customer data is stored within each Customer's exclusive tenant within AWS. Customers can decide whether its tenant will be located in Europe or the United States.

Zuora has offices located throughout the United States, Europe, and APAC. To provide Customers with comprehensive support, Zuora uses "follow the sun" approach for staffing its technical and support teams. A Customer may choose to have its tenant hosted and data stored exclusively within European Union. However, Zuora personnel in the United States and APAC may provide support and technical assistance.

By design, the Services specifically limit access to Customer's data (and especially personal data) by including self-help tools that enable each Customer to manage data stored in their tenant. Zuora will provide assistance with using its Services and performs regular maintenance and updates to ensure that its Services are functioning appropriately. Further, Zuora follows Privacy By Design principles when providing its Services which includes limiting any access to a Customer's data to only that individual(s) necessary to perform the Services. Zuora does not need to access a Customer's tenant in order to perform these functions.

What technical measures does Zuora have in place to protect Customer's personal data within the Services?

We understand that data protection requires a robust and technically secured environment. Zuora has implemented appropriate data protection and security measures throughout its organization, including affiliates, and requires third-party suppliers (subprocessors) to commit to meet the same or greater security standards.

Zuora encrypts data-in-motion using either TLS, AES-256, or FIPS depending on its sensitivity and location. Zuora also employs logical data separation at the application level. Each of our Customer's instances is assigned its own tenant identification ("**Tenant ID**") which is encrypted and embedded in the session identifier and gets validated before granting access to the user. Database tables include the Tenant ID as an identifier to logically segregate tenant specific information. Zuora also performs continuous penetration testing to verify tenant level crosstalk vulnerabilities do not exist and that the application-level tenant segregation is effective.

A copy of our technical and organizational measures, policies and procedures, and evidence of our certifications are made available to current Customers upon request.

How is access to the Services managed?

Customers can assign different levels of access to their users. The Services also allow Customers to assign permissions based on the user's role. Zuora has committed to provide assistance to any Customer with managing personal data in its tenant. Our Customer commitment is described in the master subscription and data protection agreements.

Zuora makes a contractual commitment to Customers that its personnel may only access personal data in accordance with the Customer's documented instructions for a specific purpose, such as (1) delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences; (2) troubleshooting (preventing, detecting, and repairing problems); (3) ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, quality, and security); and (4) certain "**business operations**" incident to delivery of the Services to

Customer (billing and account management; internal reporting; combatting fraud, cybercrime, or cyber-attacks that may affect Services; improving the core functionality of accessibility, privacy or efficiency of Services; and compliance with legal obligations). When processing for its business operations, Zuora will apply principles of data minimization and will not use or otherwise process Customer's personal data for: (A) user profiling, (B) advertising or similar commercial purposes, or (C) any purpose other than for the purposes set out in the master subscription agreement.

What is Zuora's position on responding to a government demand to access a Customer's data?

All companies in the U.S. are required to comply with applicable laws, but this does not mean that the U.S. government can obtain unfettered access to data processed by U.S. companies. In fact, data access laws in the U.S. are not dissimilar from those in many other countries (including those in the European Union), such that any government access to data is subject to a rigorous review and approval processes. Such laws also recognize the right of companies to challenge requests for data, for example, because the requests are overly broad, or may conflict with another country's laws or national interests.[1]

If an agency or authority demands access our Customer's data, Zuora will redirect the requestor to make the request directly to the Customer. If redirecting the requestor is not an option, Zuora will provide the Customer with reasonable notice of the demand to allow the Customer to take such other steps that it deems appropriate.

If Zuora is unable to provide a Customer with notice, we will independently review the adequacy of the request and, as appropriate, take measures to challenge its terms. Zuora will also promptly notify Customer of its actions and/or provide it with a copy unless legally prohibited from doing so.

If Zuora is compelled by a valid and binding legal request to disclose Customer data, Zuora will only provide the minimum amount of data within the specific scope of the request. As applicable, Zuora contracts with each of its vendors who have access to personal data to require them to abide by these same requirements.

SECURITY CONTROLS & CERTIFICATIONS

Zuora Services include a variety of security controls, policies and procedures, as further described in our Service documentation.

Zuora maintains controls, policies, procedures, and processes that meet the standard of the following compliance certifications:

- Payment Card Industry Data Security Standards (PCI DSS);
- SOC 1 Type 2 and SOC 2 Type 2; and
- ISO 27001 and 27018.

[1] In response to Schrems II, the several U.S. agencies, including the United States Department of Justice (collectively, "Agencies") issued a response to the Schrems II decision. The Agencies noted that current U.S. legal safeguards ensure that U.S. intelligence agencies' access to data is based on clear and accessible legal rules, such as proportionate access to data for legitimate purposes, supervision of compliance with those rules through independent and multi-layered oversight structure. Further, these systems include remedies for violations of rights. *See White Paper: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data*.

Zuora's compliance with the above requirements is audited by an independent third- party auditor on an annual basis.[2] Zuora will provide evidence and documentation upon request.

TRANSFER IMPACT ASSESSMENT

Zuora processes Customer's data in the following countries: Australia, China, France, Germany, India, Italy, Japan, Singapore, Sweden, Switzerland, United Kingdom, and United States. As of the date of this FAQ, Zuora has no reason to believe that the laws and practices in any third country of destination (as such phrase is used in the GDPR) applicable to its processing of personal data, including any requirements to disclose personal data or measures authorizing access by a government agency or a supervisory authority, prevent Zuora from fulfilling its obligations under its master subscription or data protection agreements.

If Zuora reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its processing of personal data ("**Local Laws**") prevent it from fulfilling its obligations, it shall promptly notify the Customer. In such a case, Zuora shall use reasonable efforts to make available to the affected Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer in accordance with the master subscription and data protection agreements.

[2] Zuora continues to comply with the requirements of the EU-US Privacy Shield and the Swiss-US Privacy Shield, both of which are still recognized by the United States.