SimpleSet

DATA PROCESSING ADDENDUM

Introduction

This Data Processing Addendum (“DPA”) applies when 329Design Inc. (“329Design”, “we” or “us”) processes personal data that is subject to the General Data Protection Regulation (GDPR) on behalf of an organization or person (“Customer”) who has subscribed to one of 329Design’s solutions (the “Products”).

This DPA is incorporated into and is part of the Terms of Service (the “TOS”) for the Products. Capitalized terms not defined in this DPA are defined in the TOS.

329Design may amend this DPA from time to time, with or without prior notice. The amended DPA will become effective when posted.

Terminology

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

"Customer Personal Data" means Personal Data in Customer data.

"Data Protection Laws" means all laws and regulations applicable to the Processing of Customer Personal Data, including, as applicable: (i) the Personal Information Protection and Electronic Documents Act (Canada) (“PIPEDA”), (ii) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("CCPA"), (ili) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iv) the Swiss Federal Act on Data Protection ("FADP"), (v) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

"EEA" means European Economic Area.

"Personal Data" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

"Processing" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Restricted Transfer" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

"Schedules" means one or more schedules incorporated herein. The default Schedules for this DPA are:

Schedule 1 Cross-Border Transfer Mechanisms
Schedule 2 Region-Specific Terms

"Security Incident" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Provider.

"Specified Notice Period" is within 48 hours.

"Subprocessor" means any third party authorized by Provider to Process any Customer Personal Data.

Scope

Roles

The Customer will act as the “Controller”, i.e. the party who determines the purposes and means of the Processing of Personal Data. 329Design will act as the “Processor” of this information, being the service provider who Processes Personal Data on behalf of the Customer. Each party will comply with the provisions of Data Protection Laws that apply to its respective role as either Controller or Processor.

Scope

This DPA applies to 329Design's Processing of Personal Data under the TOS to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the TOS unless otherwise required by Data Protection Laws.

Duration

Each party will Process Personal Data only as necessary for the provision and use of the Products, and for as long as the Customer has a valid paid subscription to the Products.

Categories of Personal Data

The categories of Personal Data to be Processed will be determined by the Customer, and may include the following: name, address, email address, telephone number, company name, billing information and data concerning health. The categories of individuals whose Personal Data may be processed include the following: employees, contractors and clients of the Customer.

Obligations

329Design will:

(i) Process Personal Data only on the written instructions of the Customer. 329Design's TOS and the DPA are the Customer's written instructions for this purpose. The Customer warrants that it is and will remain authorized to give these instructions, as well as any future instructions regarding the Processing of Personal Data, and that the Customer's instructions will comply with the Data Protection Laws;

(ii) not transfer Personal Data to a country outside the European Union, the EEA or the United Kingdom, except where such third country provides appropriate safeguards by way of an adequacy decision or where the recipient of the Personal Data provides appropriate safeguards through adherence to an approved certification framework, Standard Contractual Clauses or binding corporate rules, or other legal mechanisms are in place to safeguard the Personal Data being transferred;

(iii) ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iv) implement and maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of the Personal Data (including, but not limited to, pseudonymization, encryption, incident management, restoration and access controls), and will regularly monitor compliance with these measures;

(v) use only Subprocessors who maintain at least the same level of security measures and adequate safeguards as required under this DPA and who have entered a written agreement, electronic or otherwise, with 329Design requiring such measures and safeguards. We will inform the Customer of any intended changes to its Subprocessors. If a Subprocessor fails to fulfill its data protection obligations, 329Design will be liable for the performance of such obligations;

(vi) notify the Customer, within the Specified Notice Period, after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed by 329Design, and

take all steps reasonably within 329Design's control to mitigate and remediate the breach;

(vii) meet its obligations under Data Protection Laws to assist the Customer, insofar as this is possible and at the expense of the Customer, to:

- respond to individuals' requests to exercise their rights with respect to their Personal Data being Processed by 329Design, provided however, that 329Design will not respond directly to any individual; and
- meet the Customer's legal obligations with respect to breach notification, data protection impact assessments, or the cooperation or prior consultation with a supervisory authority with respect to Personal Data Processed by 329Design;

(viii) upon request of the Customer, either delete or return Personal Data after completion of Services relating to the Processing, subject to any legal or regulatory obligations to maintain or store the Personal Data; and

(ix) provide the Customer with all information necessary to demonstrate 329Design's compliance with Data Protection Laws, and contribute to audits or inspections to be conducted by or on behalf of the Customer no more than once in any calendar year, unless an additional audit is required by Data Protection Laws or regulatory authority, or is reasonably necessary due to genuine concerns regarding our compliance with this DPA. The Customer will provide reasonable advance notice of any audit and will abide by 329Design's reasonable security requirements. 329Design may charge for any time expended for such audit or inspection at our then-current hourly rates.

Customer Obligations

Customer will be responsible:

(i) for reviewing the information made available by 329Design relating to data security and making an independent determination as to whether the Products meets Customer's requirements and legal obligations under Data Protection Laws; and

(ii) for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

Cross-Border Transfers/Region-Specific Terms

329Design (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Products.

If 329Design engages in a Restricted Transfer, it will comply with Schedule 1 (Cross-Border Transfer Mechanisms).

To the extent that 329Design Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 2 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

This DPA was last updated October 16, 2023.

Schedule 1: Cross-Border Transfer Mechanisms

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the DPA.

   1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

   1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

2. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

   2.1. The EU SCCs are hereby incorporated by reference as follows:

   (a) Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Provider is a Processor of Customer Personal Data;

   (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and Provider is a Processor of Customer Personal Data;

   (c) Customer is the "data exporter" and Provider is the "data importer"; and

   (d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

   2.2. For each Module, where applicable the following applies:

   (a) the optional docking clause in Clause 7 does <u>not</u> apply;

   (b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA;

   (c) in Clause 11, the optional language does <u>not</u> apply;

   (d) in Clause 13, all square brackets are removed with the text remaining;

   2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

   3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 1 with the following modifications:

(a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

(b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;

(c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;

(d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and

(e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 1 with the following modifications:

(a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

(c) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 1;

(d) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(e) in Part 2: Part 2 - Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

Schedule 2: Region-Specific Terms

A. **CALIFORNIA**

1. Definitions. CCPA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA.

2. **Obligations**.

2.1. Customer is providing the Customer Personal Data to Provider under the Agreement for the limited and specific business purposes of providing the Cloud Service as described to this DPA and otherwise performing under the Agreement.

2.2. Provider will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

2.3. Provider acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Provider's use of Customer Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from Provider notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

2.4. Provider will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

2.5. Provider will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 2 or (ii) outside of the direct business relationship between Provider with Customer, except, in either case, where and to the extent permitted by the CCPA.

2.6. Provider will not sell or share Customer Personal Data received under the Agreement.

2.7. Provider will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

3. **Activity Prior to January 1, 2023**. To the extent this Section A (California) of Schedule 2 is in effect prior to January 1, 2023, Provider's obligations hereunder that are required solely by amendments to the CCPA made by the California Privacy Rights Act regarding contractual obligations of service providers shall only apply on and after January 1, 2023.