



SITECORE’S ONLINE CUSTOMER DATA PROCESSING ADDENDUM – GUIDANCE DOCUMENT

As global privacy and data protection legislation regimes continue to evolve, we want to help our customers address their compliance obligations. Therefore, we ensure that our Online Customer Data Processing Addendum (“DPA”) is kept current to ensure that it accurately details our obligations when handling customer personal information/personal data.

We have created this document as a resource to assist in reviewing the DPA. This is not to be construed as legal advice.

A. WHAT IS THE DPA?

Why do we use Sitecore’s DPA?

Sitecore’s DPA is specifically tailored to Sitecore’s products and services, and when executed, ensures alignment with the privacy laws and data protection regulations for new and existing customers. This DPA also captures the relevant flow-down provisions between Sitecore and its Subprocessors (such as Microsoft Azure and Amazon AWS).

What is the purpose of this DPA?

This DPA contains all relevant information regarding the processing of Customer Data in the provision of Sitecore’s product and services. This DPA includes:

| | |
|--------------------|--|
| Definitions | The important terms involved in the DPA are set out here to ensure that our customers can clearly understand all technical and legal terms that are required of a DPA |
| Terms | The obligations and commitments between Sitecore and the Customer as required by applicable Data Protection Laws and Regulations (including the GDPR, CCPA, UK Data Protection Act, Swiss FADP). |
| Annexes | <p>These annexes include:</p> <ul style="list-style-type: none">• Technical and Organizational Security Measures for how Customer Data is kept secure• Subprocessors• Data Processing• Mechanisms for Lawful Cross-Border Personal Data Transfers. <p>The purpose of this information is to provide transparency in the data that Sitecore processes and details the controls in place for how Sitecore complies with applicable regulations.</p> |

| | |
|---|--|
| 1. Standard Contractual Clauses (“SCCs”) | To the extent applicable, Model Clauses may be used in order to achieve an adequate mechanism for lawful cross-border personal data transfers. The available model clauses include European Standard Contractual Clauses, UK International Data Transfer Addendum, and a Swiss Addendum to the Standard Contractual Clauses. |
|---|--|

1. Which modules of the Standard Contractual Clauses have been used?

| | |
|--|--|
| EU | Sitecore, as the processor of Customer Data, has adopted Module Two: Controller to Processor of the EU Standard Contractual Clauses. |
| UK International Data Transfer Addendum | UK International Data Transfer Addendum supplements the Standard Contractual Clauses to provide appropriate safeguards for transfers of personal data in compliance with section 119(A) and article 46 of the UK Data Protection Act 2018. |
| Swiss Addendum to the SCCs | Swiss Addendum to the Standard Contractual Clauses supplements the Standard Contractual Clauses to provide appropriate safeguards for transfers of personal data in compliance with the Swiss Federal Act on Data Protection 1992 (“FADP”) . EU model clauses have been modified to permit Swiss to ex-Swiss transfers, in accordance with the guidance provided by the Swiss privacy regulator here . |

B. HOW TO COMPLETE THE DPA?

Who should execute this DPA?

The the DPA details the obligations of the parties when data is being collected and processed as part of any Services Agreement with Sitecore. This DPA is therefore applicable for **all customers of Sitecore Cloud and SaaS Services** (which includes Managed Cloud, EXM, Sitecore Content Hub, Sitecore Discover, Sitecore Search, Sitecore Send, Sitecore, AI, Sitecore CDP, Sitecore Ordercloud, Sitecore Personalize, Sitecore Experience Manager, and Sitecore Experience Edge.)

This DPA, which has been drafted to reflect the requirements of applicable data protection laws including GDPR, UK Data Protection Act 2018, CCPA and the FADP.

How to Execute this DPA

The Online DPA is incorporated by reference within the Agreement for services and once the Agreement is executed the terms of the online DPA will be binding as of the effective date of the Agreement.

C. WHERE CAN I GO WITH QUESTIONS?

Further information

For further information on Sitecore’s privacy and data protection practices, please visit our **Trust Center** at www.sitecore.com/trust.

Contact

If you have any specific privacy queries or have any questions in relation to this DPA, please contact us at privacy@sitecore.com

| Topic | Regulatory Requirements included within the DPA | Sitecore Data Processing Addendum |
|--|---|---|
| Definitions | The CCPA and GDPR both use terminology to cover those who are subject to and bound by the relevant legislation. | <p>Section 1 provides definitions of key terms applicable to relevant data protection legislation. This includes the use of:</p> <p>Personal Data / Personal Information as analogous terms. Data Controller, Business as analogous terms. Data Processor, Service Provider as analogous terms. Subprocessor, Subservice Provider as analogous terms. Data Subject, Consumer as analogous terms.</p> |
| Scope and description of processing | The scope of the processing operations, including the subject matter, type of personal data, categories of data subjects and the duration of processing. | Sections 2 and 3 describe how the Sitecore DPA applies throughout the entire term of any Sitecore contract for Sitecore Cloud Services where personal data/information is provided to us as part of such purchased services. |
| Confidentiality | Persons authorized to process the personal data will have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. | <p>Section 3.3 (a) states that shall maintain confidentiality of Customer data.</p> <p>Section 5.3 describes how personal data/information is only shared with personnel on a need-to-know basis and those that do have access to it are subject to a duty of confidentiality.</p> |
| Do not sell personal data | The CCPA places restrictions and notice obligations on personal data sales and disclosures for a business purpose. | Section 3.3 (c) provides that Sitecore does not engage in the “sale” of personal data of California consumers. |
| Customer instructions | Processors will only process personal data upon documented instructions from the controller. | Section 3.4 (c) documents that Sitecore shall only handle your data to provide the purchased Sitecore Cloud Services and solely in accordance with your instructions as reflected in our DPA, security policies and any other applicable agreements. |
| Subprocessor | <p>Processor shall not engage another processor without prior specific or general written authorization of the controller.</p> <p>Processor only engages subprocessors by providing you with prior notice (giving you the opportunity to object).</p> <p>Subprocessor shall be bound by the same obligations as between Sitecore and its customers. Sitecore will be fully liable to its customer for any subprocessor’s failure to fulfil its data protection obligations.</p> | <p>Section 4 describes our use of both Sitecore affiliates and external service providers for some of our Sitecore Cloud Services offerings and our responsibilities when engaging them to provide services that form part of Sitecore Cloud Services offerings.</p> <p>Annex B provides a current list of Sitecore’s current subprocessors and future changes shall be documented on our website. The list is separated by product (subprocessors for each product).</p> |
| Security | Processors must maintain a security framework that meets privacy laws and best practices standards. | Section 5 details Sitecore’s commitment to maintain appropriate technical and organizational security measures to protect Customer Data. Sitecore |

| | | |
|--|--|--|
| | | maintains several security certifications, including ISO27001 and SOC2 reporting, further detail available on our Trust Center . |
| Incident management and breach notification | Processors shall maintain a personal data breach notification program and can also assist controllers to meet their own personal data breach notification duties to both regulators and data subjects. | Section 5.6 informs Sitecore’s customers about the process Sitecore has implemented to help detect and respond to security incidents involving Personal Data. |
| Provides instructions on the transfer of data | Stipulations regarding transfers of personal data to a third country or an international organization are to be documented. | Section 7 states that personal data will only be transferred in accordance with approved mechanisms including the Standard Contractual Clauses and the International Data Transfer Addendum (appended to Sitecore DPA as Annex D). |
| Data Retention and Deletion | Processors will provide detail about how controllers can have data returned to you or deleted following termination of the services. | Section 8 describes how Sitecore will retrieve data for Sitecore Cloud Services, upon Customer request, for retrieval upon termination of your Sitecore Cloud Services, followed by a data wipe so that it is unrecoverable. |
| Cooperation | Processors will assist controllers in ensuring compliance with their own privacy requirements. | Section 9 describes how Sitecore will assist its customers’ own compliance efforts, including in the following areas: <ul style="list-style-type: none"> • Notification to supervisory authorities • Notification to data subjects • Prior consultation with supervisory authorities • Assisting with DPIAs |
| Assistance with data subject rights | Controllers will assist processors with subject access and other data privacy access requests under applicable privacy laws. | Section 9 states that Sitecore will reasonably assist Customers to respond to any subject access requests or other privacy access request and will not respond to any direct requests without Customer’s prior authorization. |
| Compliance, Reports and Audits | Processors will assist controllers with audits and inspections and provide you with any information necessary to demonstrate compliance with privacy laws, including records of processing. | Section 6 describes how Sitecore will assist with audits and inspections, and the information we can provide, to demonstrate compliance with applicable laws. Section 10 Provides information on our internal compliance measures including our use of risk assessments, internal reviews, and designated contact individual Section 11.1 -11.3 Describes how Sitecore will maintain the records required and share the necessary documentation to demonstrate compliance |
| Infringements | Processors will inform Controllers of possible infringements. | Section 11.4 advises that Sitecore will notify its Customers if it becomes aware of any possible violation of the DPA. |