Data Processing Addendum

Last updated September 2024

This Data Processing Addendum, including all schedules attached hereto, (this "DPA") is incorporated into and forms part of the Formstack Software Services Agreement (the "SSA") and Sales Order(s) (together, the "Agreement") entered into by and between Customer and Formstack, LLC ("Formstack") (collectively, the "Parties"). This DPA shall apply to the extent that Formstack Processes (as defined below) Personal Data on behalf of Customer or Customer Affiliates in connection with the provision of the Services and shall be effective as of the date of Customer's acceptance ("DPA Effective Date").

By signing this DPA, the signing Customer entity enters into this DPA on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Affiliates, if and to the extent Formstack Processes Personal Data for which such Affiliates qualify as the entity that determines the purposes and means of the Processing (any such affiliate, an "Customer Affiliate"). For the purposes of this DPA only, the term "Customer" shall include Customer and Customer Affiliates.

HOW TO EXECUTE THIS DPA

This DPA has been pre-signed by Formstack. To complete this DPA, Customer must:

- Complete the information in the signature block for Customer and execute this DPA on behalf of Customer; and
- Accept the DPA via executable link OR send the executed DPA by email to legal@formstack.com; in either case, expressly indicating the name of the Customer signing this DPA.

Upon receipt by Formstack of a validly complete DPA, this DPA will become legally binding and shall supersede any previous DPAs between the Parties as it pertains to Processing Personal Data.

INTERACTION WITH THE AGREEMENT

This DPA supplements the Agreement with respect to any Processing of Personal Data by

Formstack on behalf of Customer, as amended from time to time by written agreement between the Parties. In the event of any conflict between this DPA and the Software Services Agreement, the terms of this DPA shall prevail as they relate to the Processing of Personal Data.

Formstack and the Customer agree as follows:

1. DEFINITIONS

Any capitalized terms not defined herein shall have the meaning set out in the GDPR or will have the meaning given to them in the Agreement.

> “Controller” means the Formstack Customer that is a party to this Agreement.
>
> “CCPA” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations, and amendments thereto, including the California Privacy Rights Act (CPRA).
>
> “Data Protection Law(s)” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States, applicable to Formstack’s Processing of Personal Data under the Agreement as amended from time to time.
>
> “GDPR” means both (1) the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and (2) the United Kingdom General Data Protection Regulation as defined in Section 3 of the Data Protection Act 2018 (UK GDPR).
>
> “Personal Data” means any information Formstack Processes for the Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Formstack’s possession or control, and (b) the relevant Privacy and Data Protection Laws otherwise define as protected personal information.
>
> “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
>
> “Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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 the entity which Processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means Module Two (controller to processor) annexed to Commission Implementing Decision (EU) 2021/914.

“UK Addendum” means the international data transfer addendum to the European Commission’s standard contractual clauses for international data transfers issued under Section 119A of the Data Protection Act 2018 and entered into force on 21 March 2022, as currently established.

2. ROLES AND RESPONSIBILITIES.

2.1 *Roles of the Parties.* The Parties agree, regarding the Processing of Personal Data under relevant Data Protection Laws and this Agreement, that (i) Customer determines the scope, purposes and means of Processing and is the Controller and (ii) Formstack is a Processor Processing Personal Data on Customer’s behalf. Each Party will comply with its applicable obligations under Data Protection Laws. Formstack shall Process Personal Data on Customer’s documented instructions, including with regard to transfers to a third country or international organization, unless otherwise required by applicable law, in which case Formstack will inform Customer of that requirement unless prohibited on important grounds of public interest. Each Party agrees that it will notify the other Party upon determining that it can no longer comply with relevant Data Protection Laws.

2.2 *Right to Process*. As between Customer and Formstack and except as otherwise provided for herein, (i) Customer owns all rights, title, and interest in and to Personal Data, (ii) Personal Data shall remain the property of Customer, and (iii) the Customer retains control of the Personal Data. Customer agrees that it is duly mandated to enforce the terms of this DPA on behalf of any Customer’s Affiliates, and to act on behalf of any Customer Affiliates, in the administration and conduct of any claims arising in connection with this DPA. The Customer warrants that it has all the necessary rights to provide the Personal Data to Formstack for Processing to be performed under the Agreement and remains solely responsible for its compliance obligations under the applicable Data Protection Laws, including providing any required notices and obtaining any required consents, and for the Processing instructions it gives to Formstack.

3. FORMSTACK’S PROCESSING OF PERSONAL DATA. Formstack will allow Processing of the Personal Data by its Sub-Processors as set forth in Section 5. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule A (Details of the Processing) to this DPA.

4. DATA SUBJECT RIGHTS. In the event any data subject request is made directly to Formstack

in connection with Formstack’s Processing of Personal Data, Formstack will promptly inform Customer and provide details of the same, to the extent legally permitted. If Customer has access to the relevant Personal Data, Customer must respond to the data subject request. Formstack will provide commercially reasonable efforts to assist Customer in responding to such data subject request if legally permitted or required under relevant Data Protection Laws, upon written request.

5. SUB-PROCESSORS.

5.1 *Authorization.* Customer provides general authorization for Formstack to utilize its Sub-Processors to Process any Personal Data and shall be liable for the acts and omissions to the same extent as if Formstack was performing the Services. A list of Formstack’s current Authorized Sub-Processors (the “List”) is available to Customer at https://trust.formstack.com/. Such List may be updated by Formstack from time to time. Customer agrees to subscribe to updates to the List and receive notifications (which may include but are not limited to email notifications) of new Sub-Processors, as applicable. If Customer does not subscribe to such notifications, Customer waives any right it may have to receive prior notice of changes to Sub-Processors.

5.2 *Controller Objection.* Customer may object in writing to any additional or replacement Sub-Processor, provided that such objections are based on reasonable data protection grounds, and made within ten (10) business days after receipt of the notice. If Customer objects on reasonable data protection grounds, Customer and Formstack will discuss commercially reasonable alternatives in good faith. If no resolution is reached, either Party has the right to terminate with respect to only those Services that cannot be provided by Formstack without the use of the objected to additional or replacement Sub-Processor, by providing written notice to Formstack. If Customer does not object to a Sub-Processor, then it hereby provides specific authorization to Formstack's use of such Sub-Processor for the purposes of providing services under this Agreement.

5.3 *Processing Obligations.* Formstack will ensure that Sub-Processors are aware of Processing obligations under this DPA.

6. SECURITY. Pursuant to Article 32 of GDPR, both Parties will implement and maintain appropriate technical and organizational measures in relation to its Processing of Personal Data to ensure a level of security appropriate to the risk. Such security measures are detailed in Schedule A (Details of Processing). Further to the Software Services Agreement, Customer is solely responsible for reviewing the Services, including Schedule A, to determine whether they satisfy Customer’s requirements and legal obligations. For the avoidance of doubt, Customer is responsible for its use of the Services, including protecting the security of its data and information, taking appropriate steps to securely encrypt and/or backup any data and

information Customer uploads to the Services, and properly configuring the Services and using available features and functionalities to maintain appropriate security. Customer shall ensure that it has implemented and maintains security protection and adequate backup and recovery for any data and information Customer uploads to the Services.

7. AUDIT AND COOPERATION. Upon Customer’s written request (which shall not occur more than annually, unless required by law), Formstack shall provide Customer with a confidential verification of the adequacy of its security measures and other information necessary to demonstrate Formstack’s compliance with this DPA. The report will constitute Formstack’s Confidential Information under the confidentiality provisions of the Agreement. The Parties may, if a Supervisory Authority requires, agree to appoint a third-party auditor to verify the adequacy of Formstack’s security measures. The cost of any third-party audit will be borne by Customer, unless the audit demonstrates that Formstack is not materially complying with its obligations hereunder. The third-party auditor shall not be any company that is a competitor to Formstack, and audits shall be conducted in a manner so as to minimize the impact on Formstack’s business operations. Formstack shall provide reasonable assistance to Customer to comply with requests or demands from relevant Supervisory Authorities.

8. PERSONAL DATA BREACH. Formstack will notify Customer, without undue delay, upon becoming aware of a Personal Data Breach, and in any case, no more than seventy-two (72) hours of becoming aware of such Personal Data Breach. Formstack agrees to provide Customer with information regarding mitigation actions and actions taken to minimize the extent of the Personal Data Breach, to the extent available, and relevant to Customer fulfilling its obligations as applicable under Data Protection Laws. In any event, Customer will be responsible for notifying Supervisory Authorities and/or concerned Data Subjects (where required by Data Protection Laws). Any action or notification taken by Formstack in accordance with this clause shall not be interpreted or construed, in any manner, as an admission of liability, wrongdoing, or fault.

9. TERM AND TERMINATION. This DPA shall take effect on the DPA Effective Date and continue in full force and effect until the later of (i) termination or expiry of the Agreement; or (ii) when Formstack stops Processing Personal Data.

10. EU, UK, AND SWISS CUSTOMERS.

10.1 *EU, UK, and Swiss Transfers.* In the event Processing requires a valid Transfer Mechanism, Customer (as the “data exporter/controller”) and Formstack (as the “data importer/processor”) hereby enter into (i) Standard Contractual Clauses in respect of any Restricted Transfer from Customer to Formstack governed by GDPR; (ii) the UK Addendum in respect of any Restricted Transfer from Customer to Formstack governed by UK Data Protection Law; and/or (iii) the Swiss Addendum insofar as a Restricted Swiss Data Transfer is undertaken by the Parties. Customer authorizes Restricted Transfers that are subject to the Module 2 SCC or the UK Addendum to the SCCs or the Swiss Addendum (as appropriate), and the relevant provisions of the same are incorporated by reference.

10.2 *Standard Contractual Clauses.* For the purposes of the Standard Contractual Clauses:

10.2.1 The Parties' details shall be the Parties and their Affiliates to the extent any of them is involved in such transfer.

10.2.2 The option under clause 7 shall not apply.

10.2.3 The Parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) shall be provided by Formstack to Customer only upon Customer's written request.

10.2.4 For the purposes of clause 8.6(a), Customer is solely responsible for making an independent determination as to whether the technical and organizational measures set forth in Schedule A meet Customer's requirements and agrees that the security measures and policies implemented and maintained by Formstack provide a level of security appropriate to the risk with respect to its Personal Data.

10.2.5 The Parties agree that the audits described in clause 8.9 shall be carried out in accordance with Section 7 of this DPA.

10.2.6 Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Formstack has the Customer's general authorisation to engage Sub-Processors in accordance with Section 5 of this DPA. Formstack shall make available to Customer the current list of Sub-Processors in Schedule B of this DPA.

10.2.7 Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Formstack may engage new Sub-Processors as described in Section 5 of this DPA.

10.2.8 Formstack's liability under clause 12(b) shall relate to damage caused by Formstack's failure to comply with its obligations under GDPR as it pertains to Processing of Personal Data or where it has acted outside or contrary to lawful instruction of Customer, as specified in Article 82 GDPR.

10.2.9 The governing law for the purposes of clause 17 shall be the law that is designated in the governing law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom. The courts under clause 18 shall be those designated in the venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the Parties agree that the courts of either: (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses.

10.3 *UK Addendum.* For the purposes of the UK Addendum:

10.3.1 Table 1 of the UK Addendum: (a) the Parties’ details shall be the Parties and their affiliates to the extent any of them is involved in such transfer, and (b) the Key Contacts shall be the contacts set forth in Schedule A.

10.3.2 Table 2 of the UK Addendum: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties as detailed in section 16.5.

10.3.3 Table 3 of the UK Addendum: Annex 1A, 1B, II, and III shall be set forth in Schedules A and B below.

10.3.4 Table 4 of the UK Addendum: Either Party may end this Addendum as set out in Section 19 of the UK SCCs.

10.4 *Swiss Addendum.* For purposes of the Swiss Addendum:

10.4.1 The term EU Member State or Member State shall include Switzerland.

10.4.2 To the extent legally permitted, the transfer of Personal Data shall be governed by the GDPR.

10.4.3 The provisions of the Swiss Federal Act on Data Protection of 19 June 1992 and its Ordinances (the “FADP”) are additionally applicable, in which case references to the GDPR shall be understood to be referring to the equivalent provisions of the FADP as in force from time to time, mutatis mutandis.

10.4.4 Where an international transfer of Customer Personal Data is subject to any law that protects legal entities as data subjects, the parties agree that the SCCs will apply to data relating to legal entities.

10.4.5 The Swiss Federal Data Protection and Information Commissioner shall be the competent supervisory authority with regard to the transfer of Personal Data from Switzerland.

10.5 *Changes.* If, at any time, a Supervisory Authority or a court with competent jurisdiction over a Party mandates that transfers of Personal Data from Controllers in the EEA, Switzerland or the UK (as applicable) to Processors established outside the EEA, Switzerland or the UK (as applicable) must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures) or that the specific mechanism for international transfers is deemed modified, revoked, or held to be invalid, the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted with the benefit of such additional safeguards or to pursue a suitable alternative mechanism that can lawfully support the transfer.

10.6 *Precedence.* In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. In the event of any conflict or inconsistency between the body of this DPA and the UK Addendum, the UK Addendum shall prevail. In the event of any conflict or inconsistency between the body of this DPA and the Swiss Addendum, the Swiss Addendum shall prevail.

11. CALIFORNIA CUSTOMERS.

For the purposes of this DPA, to the extent any Processing is subject to the CCPA (and any further amendments thereto), capitalized terms used in this DPA have the meaning given to them as set forth herein as well as the CCPA and Processing shall be further subject to provisions set forth herein.

11.1 *Definitions.*

“Data Protection Law” shall expressly include the CCPA.

“Data Subject” shall include “Consumer” as defined under the CCPA.

“Personal Data” shall include “Personal Information” as defined under the CCPA.

11.2 *Roles of the Parties.* Formstack acknowledges and agrees that it will Process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Formstack shall (a) not “sell” or “share” (as defined by the CCPA) Personal Data; (b) not collect, retain, use, or disclose Personal Data for any commercial purpose (as defined by the CCPA) other than as outlined in the Agreement (including this DPA), scope of the business relationship, or as otherwise permitted by the CCPA as applicable to service providers; (c) not retain, use, or disclose Personal Data outside of the scope of the Agreement or outside of the direct business relationship between Formstack and Customer; and (d) for the purpose of advertising and marketing, not combine the Personal Data that Formstack receives from, or on behalf of, Customer with Personal Data that Formstack receives from, or on behalf of, another party, or collects from its own interaction with a Customer. Each Party agrees that it will notify the other Party upon determining that it can no longer comply with relevant Data Protection Laws and take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data upon written notice from the other Party. If Customer discloses de-identified Personal Data to Formstack, Formstack will not attempt to re-identify any de-identified Personal Data. This DPA is Formstack’s certification, to the extent the CCPA or any other applicable Data Protection Law requires such a certification, that Formstack understands and will comply with the Processing limitations with respect to Personal

Data that are set forth herein. Each party acknowledges and agrees that the disclosure of Personal Data to the other does not constitute, and is not the intent of either party for such disclosure to constitute, a “sale” or “sharing” (as defined in the CCPA) of Personal Data, and if valuable consideration, monetary or otherwise, is being provided by either party under the Agreement, such valuable consideration, monetary or otherwise, is being provided for the rendering of Services and not for the disclosure of Personal Data.

This DPA is entered into and executed by the duly authorized representatives of the Parties and becomes a binding part of the Agreement.

Formstack LLC	Customer:
Matthew J. Gard	Signature:
Name: Matt Gard	Name:
Title: VP, Accounting	Title:
Date:	Date:
Email: legal@formstack.com	Email:

SCHEDULE A – DETAILS OF PROCESSING

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

The exporter (Controller) is Customer and Customer’s contact details and signature are as provided in the Agreement.

Data importer(s):

The importer (Processor) is Formstack and Formstack’s contact details and signature are as provided in the Agreement.

B. DESCRIPTION OF TRANSFER

Nature and Purpose of Processing

Formstack will Process Personal Data as necessary to perform the Services or pursuant to the

Agreement.

Subject Matter and Duration of Processing

The subject matter of the Processing is related to the performance of the Services pursuant to the Agreement. The duration of the Processing is for the duration of the Agreement, except where otherwise required by Data Protection Laws.

Categories of Data Subjects

Any categories of Data Subjects chosen by the Customer.

Types of Personal Data

Any category of Personal Data, which may include Special Categories of Data, chosen by the Customer.

Special categories of Personal Data (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measure.

Any type of Personal Data, including Sensitive Data, chosen by the Customer, and the organizational, technical and security measures set forth herein.

Frequency of the transfer

On a continuous basis as needed to provide the Services to Customer.

Sub-processors

For transfers to (sub-) processors, please specify subject matter, nature and duration of the Processing: as set out in Schedule B.

C. COMPETENT SUPERVISORY AUTHORITY

The data exporter’s competent supervisory authority will be determined in accordance with the GDPR, and where possible, will be the Irish Data Protection Commissioner.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

General Security and Privacy Practices

Formstack has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security, privacy and risk measures intended to protect Personal Data. Formstack employs a team of experienced professionals responsible for coordinating, maintaining, and assessing Formstack’s security, privacy, and risk programs.

Governance.

Formstack addresses cybersecurity and privacy risks in its risk management processes. Formstack also stays abreast of legal, regulatory, and industry standards for security and privacy.

Risk Assessment

Internal. Formstack conducts an annual risk assessment to identify critical assets, threats, and vulnerabilities.

Vendor. Formstack performs reasonable risk-based due-diligence on new and existing vendors Processing personal or protected data.

Access Control

Access Provisioning. Formstack’s employees and contractors will be granted access to Personal Data on a “need-to-know” basis and to carry out their jobs.

Access Rights Review. Access rights will be reviewed on a regular basis to ensure the level of access is appropriate for the staff position. Formstack will remove access immediately after termination of employment or contract.

Access to Customer Data. Formstack’s employees and contractors shall access Personal Data to provide the Services and in accordance with this Agreement, generally to troubleshoot or to assist with a Customer request for support.

Access to Data Processing and Hosting Provider. Access to Formstack’s external data hosting provider environment and system components must be explicitly granted to users and approved by management.

Physical Security

Data Processing and Hosting: Formstack uses AWS in the United States for secure data processing and hosting. For Formstack’s Salesforce Application, Formstack uses Azure in the United States. These external hosting providers meet System and Organization Control (SOC) standards verified by independent third-party examination reports demonstrating how the provider achieves key compliance controls and objectives.

Laptops: Laptops used at Formstack are protected by encryption and anti-virus.

Authentication and Passwords

Identity Management. Employees and contractors are issued unique user accounts.

Passwords. Employees and contractors are required to comply with password parameters and standards and must use multi-factor authentication when available.

Training and Awareness

Training. Employees and contractors receive privacy and security training upon hire. Additional security and privacy training are provided on an annual basis with quarterly awareness updates. Training is mandatory.

Data Security

Encryption in Transit. Formstack uses industry-standard cryptographic protocols to create secure connections for data in transit.

Encryption at Rest. The files stored and the data that resides on Formstack's databases are encrypted using industry-accepted standards and algorithms for encryption.

Key Management. Formstack will provide rules for key management to protect the lifecycle of cryptographic keys from loss or misuse.

Firewall. Formstack configures a virtual firewall within its external data hosting providers to limit service access using security groups or similar functionality.

Information Protection

Background Checks. Formstack performs criminal background checks on employees and contractors with access to data and application hosting environments, where legally permitted to do so.

Change Control. Changes to the production environment must be approved. A formal change process that includes documentation of changes, peer review, approval of changes, testing of changes prior to deployment, and auditing of changes.

System Development Lifecycle. Formstack integrates security into the system development process from the initiation of a project to develop a system to its disposition.

Secure Software Development. Formstack uses industry best practices to produce software code for its applications. Software engineers and developers are trained in secure coding techniques, avoiding common coding vulnerabilities, and understanding how sensitive data is handled.

Application Code. Formstack maintains application code at a third-party provider.

Continuous Security Monitoring

Anomalies and Events. Formstack uses intrusion detection technology, proactive risk identification and real-time threat detection to detect system changes or abnormalities.

Audit Logs. Formstack applications are configured for appropriate logging of activities to enable detection of security incidents.

Testing. In addition to real-time threat detection, Formstack runs monthly vulnerability scans on its applications. High-value issues are addressed based on severity of the problem.

Security Incident and Data Breach Response.

Incident and Data Breach. Formstack has implemented and maintains a security incident and data breach response plan for actual security incidents involving the breach of Personal Data.

Disaster Recovery and Business Continuity. Formstack maintains a DR/BC plan. With a significant number of remote employees and contractors, it is unlikely that the entirety of the organization would be impacted by a disaster.

SCHEDULE B – SUB-PROCESSORS USED BY FORMSTACK

Formstack Trust Center