Data Processing Addendum

Last Updated: October 1, 2023

This Data Processing Addendum (this "**Addendum**") supplements the underlying agreement (the "**Agreement**") entered into by and between Benchling, Inc. ("**Benchling**") and the customer entity that is a party to the Agreement ("**Customer**"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "**Application Services**," "**Benchling Services**," and "**Usage Data**" have the meanings as defined in the Agreement.

1.2 "**Authorized Subprocessor**" means any authorized third-party processor engaged by Benchling to process Customer Personal Data in order to provide the Benchling Services to Customer.

1.3 "**Account Data**" means personal data that relates to Benchling's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Account Data also includes any data Benchling may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.4 "**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 the processing of Personal Data.

1.5 "**Customer Personal Data**" means Personal Data in Customer Data (as that term is defined in the Agreement).

1.6 "**Data Protection Laws**" refers to all laws and regulations applicable to Benchling's processing of Personal Data under the Agreement.

1.7 "**Personal Data**" means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier, or one of more factors specific to that natural person.

1.8 "**processor**" means the entity which processes Personal Data on behalf of the controller.

1.9 "**processing**" (and "**process**") means any operation or set of operations 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 of, restriction, erasure or destruction.

1.10 "**Security Incident**" means the confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Customer Personal Data, transmitted, stored or otherwise processed by Benchling of which Benchling becomes aware.

1.11 "**Schedules**" means:

1.11.1 Schedule 1: Subject Matter and Details of Processing

1.11.2 Schedule 2: Technical and Organizational Security Measures

1.11.3 Schedule 3: Cross-Border Transfer Mechanism

1.11.4 Schedule 4: Region-Specific Terms

2. Relationship of the Parties; Processing of Customer Personal Data

2.1 Benchling as a Processor. The parties acknowledge and agree that with regard to the processing of Customer Personal Data, Customer may act as either a controller or processor and Benchling is a processor. Benchling will process Customer Personal Data in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions).

2.2 Benchling as a Controller of Account Data. The parties acknowledge that, with regard to the processing of Account Data, Customer and Benchling are both independent controllers. Benchling will process Account Data as a controller in order to: (a) manage the relationship with Customer, (b) carry out Benchling's core business operations, such as billing, accounting and filing taxes, (c) detect, prevent or investigate Security Incidents, fraud, and other abuse or misuse of the Benchling Services, (d) perform identity verification, (e) comply with Benchling's legal or regulatory obligations, (f) provide support and professional services, and (g) as otherwise permitted under Data Protection Laws and in accordance with this Addendum, the Agreement, and the Benchling Privacy Policy at https://benchling.com/privacy.

2.3 Benchling as a Controller of Usage Data. The parties acknowledge that, with regard to the processing of Usage Data, Customer may act either as a controller or processor and Benchling is an independent controller. Benchling will process Usage Data as a controller in order to carry out necessary functions, such as: (a) provide, optimize, improve and maintain the Benchling Services, platform and security; (b) investigate fraud, spam, wrongful or unlawful use of the Benchling Services; (c) provide support and professional services, (d) comply with Benchling's legal or regulatory obligations, or (e) as otherwise permitted under Data Protection Laws and in accordance with this Addendum, the Agreement, and the Benchling Privacy Policy at https://benchling.com/privacy.

3. Purpose Limitation. Benchling will process Customer Personal Data in accordance with the Agreement in order to provide the Benchling Services . Schedule 1 (Subject Matter and Details of Processing) further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of Personal Data and the categories of data subjects.

4. Compliance. Customer is responsible for ensuring that (a) it has complied, and will continue to comply with Data Protection Laws in its use of the Benchling Services and its own processing and sharing of Personal Data with Benchling and (b) it has, and will continue to have, the right to transfer, or provide access to, Customer Personal Data for Benchling to process in accordance with the terms of this Addendum.

5. Customer Instructions. Customer appoints Benchling as a processor to process Customer Personal Data on behalf of, and in accordance with, Customer's instructions as set forth in the Agreement, this Addendum, and as otherwise necessary to (a) provide the Benchling Services to Customer, which includes investigating and mitigating security incidents; (b) comply with applicable law or regulation, including Data Protection Laws; and (c) as otherwise agreed in writing between the parties ("**Permitted Purposes**").

5.1 Lawfulness of Instructions. Customer will ensure that its instructions comply with Data Protection Laws. Customer acknowledges that Benchling is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Benchling's provision of the Benchling Services meets or will meet the requirements of such laws or regulations. Customer will ensure that Benchling's processing of Customer Data, when done in accordance with Customer's instructions, will not cause Benchling to violate any applicable law or regulation, including Data Protection Laws. Benchling will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate any applicable law or regulation, including Data Protection Laws.

5.2 Additional Instructions. Additional instructions outside the scope of the Agreement or this Addendum will be agreed to between the parties in writing, and may include additional fees that may be payable by Customer to Benchling for carrying out such additional instructions.

6. Confidentiality. Benchling shall ensure that any person it authorizes to process Customer Personal Data has agreed to protect Customer Personal Data in accordance with Benchling's confidentiality obligations in the Agreement and this Addendum. Customer agrees that Benchling may disclose Customer Personal Data to its advisers, consultants, auditors or other third parties as reasonably required in connection with the performance of its obligations under this Addendum, the Agreement, the provision of Benchling Services to Customer and if legally required to do so.

7. Authorized Subprocessors

7.1 Authorization for Onward Subprocessing. Customer provides general written authorization to Benchling to engage onward subprocessors as necessary to perform the Benchling Services, conditioned on the following requirements:

7.1.1 Benchling will restrict the onward subprocessor's access to Customer Personal Data only to what is necessary to provide the Benchling Services, and Benchling will prohibit subprocessors from processing the Customer Personal Data for any other purpose;

7.1.2 Benchling agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect Customer Personal Data, on any subprocessor it appoints that require such subprocessor to protect Customer Personal Data to the standard required by Data Protection Laws, including requirements substantially similar to those set forth in this Addendum.

7.1.3 Benchling will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its subprocessors.

7.2 Current Subprocessors and Notification of Subprocessor Changes. Benchling maintains an up-to-date list of its subprocessors at https://benchling.com/privacy/subprocessors ("**List**"). The List may be updated by Benchling from time to time. At least ten (10) days before enabling any subprocessor other than existing Authorized Sub-Processors to access or participate in the processing of Customer Personal Data, Benchling will add such subprocessor to the List and notify Customer via email or another mechanism for notifications to which Customer has subscribed. Customer may object to such an engagement by informing Benchling within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain subprocessors are essential to providing the Benchling Services and that objecting to the use of a subprocessor may prevent Benchling from offering the Benchling Services, or an aspect of the Benchling Services to Customer.

7.3 Objection Right for new Subprocessors. Customer may object to Benchling's appointment or replacement of a subprocessor prior to such appointment or replacement, provided such objection is in writing and based on reasonable grounds related to data protection. In such an event, the parties agree to discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach a resolution within ninety (90) days from the date of Benchling's receipt of Customer's written objection, Customer may discontinue the use of the affected Services by providing written notice to Benchling. Discontinuation shall not relieve Customer of any fees owed to Benchling as of the date of termination under the Agreement. If Customer does not raise an objection prior to Benchling replacing or appointing a new subprocessor, Benchling will deem Customer to have authorized the new subprocessor.

8. Security.

8.1 Security Measures. Benchling will implement and maintain technical and organizational measures designed to protect the security and confidentiality of Customer Data, in accordance with Benchling's security measures referenced in the Benchling Information Security Policy, the current version of which is located at https://www.benchling.com/information-security-policy and as further described in Schedule 2 (Technical and Organizational Security Measures).

8.2 Determination of Security Requirements. Customer is responsible for reviewing the information Benchling makes available regarding its data security and making an independent determination as to whether the Benchling Services meet Customer's requirements and legal obligations, including its obligations under Data Protection Laws.

8.3 Security Incident Notification. Benchling will, to the extent permitted by applicable law, notify Customer without undue delay, and in no event later than seventy-two (72) hours after Benchling's discovery of any Security Incident. Benchling will make reasonable efforts to identify a Security Incident, and to the extent within Benchling's control, remediate such Security Incident. Benchling will provide reasonable assistance to Customer in the event that Customer is required under Data Protection Laws to notify a regulatory authority or any data subjects impacted by a Security Incident. The aforementioned obligations shall not apply in the event that a Security Incident results from the actions or omissions of Customer Benchling's obligation to report or respond to a Security Incident under this section will not be construed as an acknowledgement by Benchling of any fault or liability with respect to the Security Incident.

9. Deletion of Customer Data. Following completion of the Benchling Services and upon Customer's written request, Benchling shall delete Customer Data (including Customer Personal Data), unless ongoing storage of such data is required or authorized by applicable law or is impracticable. If destruction is prohibited by law, rule or regulation or is impracticable, Benchling shall take measures to block any Customer Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect such Customer Personal Data remaining in its possession, custody, or control.

10. Data Subject Requests

10.1 Assisting Customer. Benchling will, upon Customer's written request and taking into account the nature of the applicable processing, provide Customer with reasonable assistance in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection), provided that Customer cannot reasonably fulfill such requests independently (including through use of the Benchling Service).

10.2 Data Subject Requests. If Benchling receives a request from a data subject in relation to the data subject's Customer Data, Benchling will notify Customer and advise the data subject to submit the request to Customer (but not otherwise communicate regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such requests.

11. Audits

11.1 Benchling's Records Generally. Benchling will keep records of its processing in compliance with Data Protection Laws and make any necessary records available to Customer to demonstrate compliance with its obligations under Data Protection Laws and this Addendum, upon Customer's reasonable request.

11.2 Third-Party Compliance Program. Benchling uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Data. Such audits are performed at least once annually, at Benchling's expense, by independent third-party security and compliance professionals selected by Benchling, and result in the generation of a confidential audit report ("**Audit Report**"). Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Benchling will make available to Customer a copy of Benchling's most recent Audit Report. Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by such Audit Report.

11.3 Customer Audit.

11.3.1 Trigger. To the extent that Benchling's provision of an Audit Report does not provide sufficient information for Customer to verify Benchling's compliance with this Addendum or Data Protection Laws, or Customer is legally required to respond to a regulatory authority audit, Customer has the right, at Customer's expense, to conduct an audit of Benchling's data security infrastructure and procedures (an "**Audit**") pursuant to a mutually agreed-upon audit plan with Benchling that is consistent with the below Audit Parameters, defined below.

11.3.2 Audit Parameters. Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Benchling; (ii) occur at a mutually agreed date and time, only during Benchling's regular business hours, and with at least thirty (30) days prior written notice from Customer; (iii) occur no more than once annually; (iv) cover only facilities controlled by Benchling; (v) not violate any obligation between Benchling and its service providers or other third parties; (vi) restrict findings to only Customer Data relevant to Customer; and (vii) obligate Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

12. Data Transfers.

12.1 Hosting and Processing Locations. Benchling's primary hosting location is in the United States, unless Customer elects another hosting region offered by Benchling (either, a "Hosting Region"). Customer acknowledges that Benchling's primary processing activities occur in the United States, regardless of the Hosting Region.

12.2 Transfer Mechanism. To the extent Customer's use of the Benchling Services requires an onward transfer mechanism to lawfully transfer Customer Personal Data from a jurisdiction (i.e., the European Economic Area, the United Kingdom, or Switzerland) to Benchling located outside of that jurisdiction ("**Transfer Mechanism"**), the terms set forth in Schedule 3 (Cross Border Transfer Mechanism) will apply.

13. **Jurisdiction Specific Terms**. To the extent that Benchling processes Personal Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Schedule 4 (Jurisdiction Specific Terms), the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) will apply.

14. **Failure to Perform.** In the event that changes in law or regulation render performance of this Addendum impossible or commercially unreasonable, the parties may renegotiate this Addendum in good faith. If renegotiation would not cure the impossibility or the parties cannot reach an agreement, the parties may mutually agree to terminate the Agreement. Such Termination shall not relieve Customer of any fees owed as of the date of termination to Benchling under the Agreement.

15. **Updates**. Benchling may update the terms of this Addendum from time to time; provided however, Benchling will provide at least thirty (30) days prior written notice to Customers when an update is required as a result of (a) changes to Data Protection Laws; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Benchling Services.

16. **Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule 4 (Jurisdiction Specific Terms) of this Addendum; (2) the terms of this Addendum outside Schedule 4 (Jurisdiction Specific Terms); (3) the Agreement; and (4) the Benchling Privacy Policy. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Schedule 1
Subject Matter and Details of Processing

Nature and Purpose of Processing: Benchling will process Customer Personal Data as necessary to provide the Benchling Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Customer's instructions as set forth in this Addendum. The nature of processing may include, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organization and structuring
- Using data, including analysis, consultation, testing, automated decision making and profiling
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Frequency of Transfer: Benchling will process Customer Personal Data on a continuous basis for the duration of the Agreement.

Duration of Processing: Benchling will process Customer Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Benchling's legitimate business needs; or (iii) by applicable law or regulation. Account Data and Usage Data will be processed and stored as set forth in Benchling's Privacy Policy.

Categories of Data Subjects: Data subjects include the individuals about whom data is provided to the Data Importer via the Benchling Services by (or at the discretion of) the Data Exporter. This may include, but is not limited to, Customer Personal Data relating to the Customer's users, collaborators, consultants, employees, and other authorized persons.

Categories of Personal Data: As a processor, Benchling processes Customer Personal Data (including, if applicable, any Personal Data Customer collects from its end users and processes through its use of the Benchling Services) or collected by Benchling in order to provide the Benchling Services or as otherwise set forth in the Agreement or this Addendum. Categories of Personal Data include full name, title, position, IP address, browser agent, email address, user name, browser and operating system identifiers, and any other Customer Personal Data that Data Exporter chooses to send to Data Importer during the course of Data Importer's provision of the Benchling and technical support.

Sensitive Data or Special Categories of Data: None

Transfer to Subprocessors: the subject matter, nature, and duration of the processing is set forth at https://benchling.com/privacy/subprocessors.

Schedule 2
Technical and Organizational Measures

More information related to Benchling's technical and organizational security measures to protect Customer Data is available at https://www.benchling.com/trust ("**Security Overview**") and at https://www.benchling.com/information-security-policy ("**Security Policy**").

Where applicable, this Schedule 2 will serve as Annex II to the EU Standard Contractual Clauses. The following table provides more information regarding the technical and organizational measures to protect Customer Data, as set forth below:

Technical and Organizational Security Measure	**Evidence of Technical and Organizational Security Measures**
Measures of pseudonymisation and encryption of personal data	All data and communication within Benchling is protected at rest using AES 256-bit encryption, and in transit using Transport Layer Security (TLS) encryption 1.2 or higher.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Benchling maintains an information security program, which includes: (a) having a formal risk management program; (b) conducting periodic risk assessments of systems and networks that process Customer Data; (c) monitoring for security incidents and maintaining a tiered remediation plan to ensure timely fixes to any discovered vulnerabilities; (d) a written information security policy (available at https://www.benchling.com/information-security-policy) and incident response plan that explicitly addresses and provides guidance to its personnel in furtherance of the security, confidentiality, integrity, and availability of Customer Data; (e) penetration testing performed by a qualified third party on an annual basis; and (f) having resources responsible for information security efforts.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Benchling's backup policy is based on ISO-27001 standards. Benchling services are replicated to ensure high availability, redundancy, and failure tolerance. Benchling performs at least daily backups for recovery purposes. Backups are encrypted and tested at least annually.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Benchling's systems are annually subjected to a wide range of different penetration tests and external audits. The company practices "security by design" principles by incorporating threat modeling into the design phase for all key features. Any changes to Benchling's code base requires additional testing and review prior to migrating to the production environment. Security tooling is integrated into Benchling's code pipeline, which incorporates a number of checks for application security vulnerabilities, such as static code analysis, and dependency checking. In addition, members of Benchling's security team

	regularly perform manual application security testing on key components.
Measures for user identification and authorisation	Benchling systems are managed through an SSO provider which enforces multi-factor authentication. Benchling observes the principles of “least privilege” and “role based access” meaning access to data and systems are limited to what is necessary in order to fulfill an employee's current job responsibilities. Benchling utilizes segregation of duties to reduce the risk of unauthorized or unintentional modification or misuse of systems or data. Systems require user authentication and user access (including privileged access) to be reviewed quarterly or when changes to personnel occur.
Measures for the protection of data during transmission	All data and communication within Benchling is protected in transit using Transport Layer Security (TLS) encryption 1.2 or higher.
Measures for the protection of data during storage	All data and communication within Benchling is protected at rest using AES 256-bit encryption. By default, Customer Data is stored and processed within a secure cloud environment hosted on Amazon Web Services (AWS).
Measures for ensuring physical security of locations at which personal data are processed	Benchling utilizes AWS for hosting. AWS is a leader in infrastructure security, and maintains multiple security and compliance certifications including ISO 27001, SOC 1, SOC 2, and SSAE16. In addition, all Benchling offices and Benchling-managed work spaces have a physical security program that manages visitors, building entrances, closed circuit televisions, and overall office security. All employees, contractors, and visitors are required to wear an identification badge.
Measures for ensuring events logging	All key actions performed within Benchling, such as logins, data writes and configuration changes, are attributable to particular users, and are captured with user information, date and time stamps in the audit logs. Logging data is centralized where it is made available for authorized individuals to monitor and take action in the event of an incident.
Measures for ensuring system configuration, including default configuration	Benchling systems are built leveraging baseline configurations which are hardened in accordance with industry best practices like Center for Information Security (CIS).
Measures for internal IT and IT security governance and management	Benchling’s IT services are automated and compartmentalized to limit the security risk of any single component of the system. Benchling practices a “Zero Trust” policy. This means multiple security attributes are assigned to each Benchling team member and user account, and multi-factor authentication is required in order to access any of the company’s IT services. A final

	layer of security is provided by the NIST Security Risk Management Framework, in which each security risk is assessed according to a set of internal benchmarks, with significant decisions requiring confirmation from Benchling's senior executive team.
Measures for certification/assurance of processes and products	Benchling's dedicated security and privacy programs are externally audited annually. The company maintains an International Organization for Standardization (ISO) 27001 certification. All Benchling's operations comply with the General Data Protection Regulation (GDPR). In addition, Benchling aligns its security program and capabilities with the Cloud Computer Compliance Controls Catalog (C5), National Cyber Security Center (NCSC) Cloud Security Principles, and National Institute of Standards and Technology (NIST) Cloud Computing Standards.
Measures for ensuring data minimisation	Benchling only collects information that is necessary in order to provide the Services outlined in the Agreement. Our employees are directed to access only the minimum amount of information necessary to perform the task at hand.
Measures for ensuring data quality	Benchling maintains logging details that include any changes to sensitive configuration settings and files. At minimum, log entries include date, timestamp, action performed, and the user ID or the device ID of the action performed. Logs are protected from change.
Measures for ensuring limited data retention	Benchling will retain information for the period necessary to provide the Services and for a period of time thereafter in backups, unless a longer retention period is required or permitted by law, or where the Agreement requires or permits specific retention or deletion periods.
Measures for ensuring accountability	Benchling has established a comprehensive GDPR compliance program and is committed to partnering with Customers and vendors on compliance efforts. Specifically, Benchling has taken the following steps to align its practices with GDPR: (i) all employees are required to complete annual GDPR training and security training, (ii) policies and contracts are in place with our partners and vendors to comply with GDPR, (iii) we have enhanced security practices and procedures, (iv) we have implemented tools to produce data maps, (v) we have created robust internal privacy and security documentation, (vi) we have appointed a Data Protection Officer, and (vii) we have implemented tools and procedures to respond to data subject access requests.
Measures for allowing data portability and ensuring erasure	Benchling provides a mechanism for individuals to exercise their privacy rights in accordance with applicable law. Individuals request that Benchling delete their data or provide a copy of their data here.

Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	When Benchling engages a subprocessor under this Addendum, Benchling and the subprocessor enter into an agreement with data protection obligations substantially similar to those contained in this Addendum. Each subprocessor must ensure that Benchling is able to meet its obligations to Customers. In addition to implementing technical and organizational measures to protect Customer Data, the subprocessors must (a) notify Benchling in the event of a Security Incident, (b) delete Personal Data when instructed by Benchling in accordance with Customer's instructions to Benchling; (c) not engage additional subprocessors without Benchling's authorization; (d) not change the location where Personal Data is processed; and (e) not process Personal Data in a manner which conflicts with Customer's instructions to Benchling.

Schedule 3
Cross-Border Transfer Mechanism

1. **Definitions**

1.1. "**Data Privacy Framework**" or the "**DPF**" means, as applicable, the EU-US Data Privacy Framework ("**EU-US DPF**"), the Swiss-US Data Privacy Framework ("Swiss DPF"), and/or the UK Extension to the EU-US DPF (the "**UK Extension**"), under the self-certification program operated by the United States Department of Commerce.

1.2. "DPF Principles" means the Data Privacy Framework principles available at www.dataprivacyframework.gov.

1.3. "**EEA**" means the European Economic Area.

1.4. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914 on June 4, 2021.

1.5. "**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. Cross-Border Data Transfer Mechanism

2.1. Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism, as applicable, and in accordance with the following order of precedence: (a) the applicable Data Privacy Framework; (b) the EU SCCs, or (c) the UK International Data Transfer Agreement.

2.2. Data Privacy Framework. To the extent that Benchling processes any Personal Data via the Benchling Services originating from the EEA, Switzerland, or the UK, Benchling represents that it complies with the DPF Principles when processing any such Personal Data and is (or will be, when available) self-certified under the applicable DPF. To the extent that Customer is (a) located in the United States of America and is self-certified under the DPF or (b) located in the EEA, Switzerland or the UK, Benchling further agrees (i) to provide at least the same level of protection to any Personal Data as required by the DPF Principles, (ii) to notify Customer in writing, without undue delay, if its self-certification to the DPF is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative Transfer Mechanism will apply in accordance with the order or precedence set forth above) and (iii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of Personal Data.

2.3. EU Standard Contractual Clauses. In the event that the applicable DPF is invalidated or does not apply, the parties agree that the EU SCCs will apply to Personal Data that is transferred via the Benchling Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the EU SCCs, the EU SCCs will be deemed entered into (and incorporated into this Addendum by reference) and completed as follows:

2.3.1. Module One (Controller to Controller) of the EU SCCs apply when Benchling is processing Personal Data as a controller pursuant to Section 2 of this DPA.

2.3.2. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Benchling is processing Customer Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

2.3.3. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Benchling is processing Customer Personal Data on behalf of Customer as a subprocessor.

2.4. For each module, where applicable the following applies:

2.4.1. The optional docking clause in Clause 7 does apply.;

2.4.2. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 7 of this DPA;

2.4.3. In Clause 11, the optional language does not apply;

2.4.4. In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;

2.4.5. In Clause 18(b), disputes will be resolved before the courts of Ireland;

2.4.6. In Annex 1, Part A of the EU SCCs:

- Data Exporter: Customer
- Contact Details: The email address(es) designated by Customer
- Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Relationship of the Parties) of this DPA.
- Signature & Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU SCCs incorporated herein, including their Annexes, as of the effective date of the Agreement.

- Data Importer: Benchling, Inc.
- Contact Details: privacy@benchling.com
- Data Importer Role: The Data Importer's role is set forth in Section 2 (Relationship of the Parties) of this DPA.
- Signature & Date: By entering into the Agreement, Data Importer is deemed to have signed these EU SCCs incorporated herein, including their Annexes, as of the effective date of the Agreement.

2.4.7. In Annex 1, Part B of the EU SCCs:

2.4.7.1. The categories of data subjects are set forth in Schedule 1 (Subject Matter and Details of Processing).

2.4.7.2. No Sensitive Data will be transferred, as specified in Schedule 1 (Subject Matter and Details of Processing).

2.4.7.3. The frequency of the transfer is on a continuous basis for the duration of the Agreement.

2.4.7.4. The nature of the processing is set forth in Schedule 1 (Subject Matter and Details of Processing).

2.4.7.5. The purpose of the processing is set forth in Schedule 1 (Subject Matter and Details of Processing).

2.4.7.6. The period for which Customer Personal Data will be retained is set forth in Schedule 1 (Subject Matter and Details of Processing).

2.4.7.7. For transfers to subprocessors, the subject matter, nature, and duration of the processing is set forth at: https://benchling.com/privacy/subprocessors

2.4.7.8. In Annex 1, Part C of the EU SCCs, the Irish Data Protection Commission will be the competent supervisory authority; and

2.4.7.9. Schedule 2 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the EU SCCs

2.5. Switzerland Data Transfer. In the event that the Swiss DPF is invalidated or does not apply, the parties agree that, to the extent that Customer Personal Data transfers from Switzerland, are subject to the EU Standard Contractual Clauses in accordance with Section 2.1 of Schedule 3 (Cross Border Data Transfer Mechanisms), the following amendments will apply to the EU Standard Contractual Clauses:

2.5.1. References to "EU Member State" and "Member State' will be interpreted to include Switzerland, and

2.5.2. Insofar as the transfer or onward transfers are subject to the Swiss Federal Act on Data Protection (“**FADP**”):

2.5.3. References to Regulation (EU) 2016/679 are to be interpreted as references to the FADP;

2.5.4. The "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

2.5.5. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and

2.5.6. In Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland

2.6. UK International Data Transfer Agreement. In the event that the EU-US DPF (including the UK Extension) is invalidated or does not apply, the parties agree that the UK International Data Transfer Agreement will apply to Customer Personal Data that is transferred via the Benchling Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is: (a) not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Customer Personal Data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by reference) and completed as follows:

2.6.1. In Table 1 of the UK International Data Transfer Agreement, the parties key contact information is located in Section 2.2.6 of this Schedule 3.

2.6.2. In Table 2 of the UK International Data Transfer Agreement, information about the version of the EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.1 (EU Standard Contractual Clauses) of this Schedule 3.

2.6.3. In Table 3 of the UK International Data Transfer Agreement:

2.6.3.1. The list of parties is located in Section 2.2.6 of this Schedule 3.

2.6.3.2. The description of the transfer is set forth in Schedule 1 (Subject Matter and Details of Processing).

2.6.3.3. Annex II is located in Schedule 2 (Technical and Organizational Security Measures)

2.6.3.4. The list of subprocessors is located at https://benchling.com/privacy/subprocessors

2.6.4. In Table 4 of the UK International Data Transfer Agreement, both the Importer and the Exporter may end the UK International Data Transfer Agreement in accordance with its terms.

3. **Conflict**. To the extent that there is any conflict or inconsistency between the EU SCCs or the UK International Data Transfer Agreement and any other terms of this Addendum, the Agreement, or the Privacy Policy, then the provisions of the EU SCCs or UK International Data Transfer Agreement, as applicable, will prevail.

Schedule 4
Jurisdiction Specific Terms

1. California

1.1. Definitions:

1.1.1. The definition of "Data Protection Laws" includes the California Consumer Privacy Act (the "**CCPA**").

1.1.2. The definition of "Personal Data" includes "Personal Information" as defined under the CCPA.

1.1.3. The definition of "data subject" includes "Consumer" as defined under CCPA and any data subject rights set forth in this Addendum also apply to Consumer rights.

1.1.4. The definition of "controller" includes "Business" as defined under CCPA.

1.1.5. The definition of "processor" includes "Service Provider" as defined under CCPA.

1.2. CCPA Specific Provisions: Benchling will process, retain, use and disclose Customer Personal Data only as necessary to provide the Benchling Services under the Agreement, which constitutes a business purpose. Benchling will not (a) sell (as that term is defined under CCPA) Customer Personal Data; (b) retain, use or disclose Customer Personal Data for any commercial purpose (as defined under CCPA) other than providing the Benchling Services; or (c) retain, use or disclose Customer Personal Data outside the scope of the Agreement.

2. European Economic Area (EEA), Switzerland, and the United Kingdom (UK)

2.1. Definitions:

2.1.1. The definition of "Data Protection Laws" includes the General Data Protection Regulation (EU 2016/679)("**GDPR**") and all references to the GDPR will, to the extent deemed to be referenced to the corresponding laws in the UK (including the **UK GDPR** and the Data Protection Act of 2018).

2.1.2. The definition of "Data Protection Laws" includes the Swiss Federal Act on Data Protection ("**FADP**")

2.2. When Benchling engages a subprocessor under Section 7 (Authorized Subprocessors) of this Addendum, Benchling will:

2.2.1. Require any Authorized Subprocessor to protect Customer Personal Data to the standards required by Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures that meet the requirements of GDPR; and

2.2.2. Only process Customer Personal Data on terms equivalent to the EU SCCs and/or the UK International Data Transfer Agreement, as applicable.

2.3. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including either party's indemnification obligations), neither party will be responsible for any GDPR fines or UK GDPR fines issued or levied under Article 83 of the GDPR or UK GDPR, respectively, against the other party by a regulatory authority or governmental body in connection with such party's violation of GDPR.