



Data Processing Agreement

This Supplier Data Processing Agreement and its Annexes (“DPA”) reflects the parties’ agreement with respect to the Processing of Personal Data by The Supplier Company (“Supplier”, “Us”, “We, or “Our”), its Affiliates or its Sub-Processors, on behalf of Client (“Client”, “You”, or “Your”) in connection with the provision of Services under an applicable Statement of Work (collectively with the Master Services Agreement between the Parties, the “Agreement”).

This DPA is supplemental to, and forms an integral part of, the Agreement and is incorporated by reference into the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency. Capitalized terms not otherwise defined in this DPA shall have the meanings set forth in the Agreement. The term of this DPA will follow the term set forth in an applicable Statement of Work or for so long as Personal Data remains in the possession of Supplier, its Affiliates or its Sub-Processors.

1. DEFINITIONS.

- 1.1 “California Personal Information” means Personal Data that is subject to the protection of the CCPA.
- 1.2 “CCPA” means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018), or as applicable, the California Privacy Rights Act (CPRA) (effective January 1, 2023).
- 1.3 “Consumer”, “Business”, “Sell” and “Service Provider” will have the meanings given to them in the CCPA.
- 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 “Data Protection Laws” means all applicable worldwide legislation relating to data protection and data privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, superseded, repealed, consolidated or replaced.
- 1.6 “Data Subject” means the individual to whom Personal Data relates.
- 1.7 “European Data” means Personal Data that is subject to the protection of European Data Protection Laws.
- 1.8 “European Data Protection Laws” means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (“GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance (“Swiss DPA”); in each case, as may be amended, superseded, repealed, consolidated or replaced.
- 1.9 “Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).
- 1.10 “Permitted Affiliates” means any of Your Affiliates that (i) are permitted to use the Services pursuant to the Agreement but have not signed their own separate agreement with us and are not the “Client” as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.
- 1.11 “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 by us and/or Our Sub-Processors in connection with the provision of the Services. “Personal Data Breach” will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- 1.12 “Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.
- 1.13 “Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
- 1.14 “Sub-Processor” means any Processor engaged by Supplier or its Affiliates to assist in fulfilling obligations with respect to the provision of the Services under the Agreement. Sub-Processors do not include any Supplier employees.



- 1.15 “Standard Contractual Clauses” means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, as may be amended, superseded, repealed, consolidated or replaced by the European Parliament and the Council.

2. CLIENT RESPONSIBILITIES.

- 2.1 Compliance with Laws. Within the scope of the Agreement and in Client’s use of the Services, You will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to us. In particular but without prejudice to the generality of the foregoing, You acknowledge and agree that You will be solely responsible for: (i) ensuring You have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (ii) ensuring that Your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (iii) complying with all laws (including Data Protection Laws) applicable to any emails or other content You or your Participants create or send through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and email deployment practices. You will inform us without undue delay if You are not able to comply with Your responsibilities under this ‘Compliance with Laws’ section or applicable Data Protection Laws.
- 2.2 Controller Instructions. The parties agree that the Agreement (including this DPA), together with Your use of the Services in accordance with the Agreement, constitute Your complete Instructions to us in relation to the Processing of Personal Data, so long as You may provide additional instructions during the Subscription that are consistent with the Agreement and the nature and lawful use of the Services.
- 2.3 Security. You are responsible for independently determining whether the data security provided for in the Services adequately meets Your obligations under applicable Data Protection Laws. You are also responsible for Your secure use of the Services, including protecting the security of Personal Data in transit to and from the Services (including to securely backup or encrypt any such Personal Data).

3. SUPPLIER OBLIGATIONS.

- 3.1 Compliance with Instructions. We will only Process Personal Data for the purposes described in this DPA, the Agreement or as otherwise agreed within the scope of Your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to You or Your industry that are not generally applicable to us.
- 3.2 Conflict of Laws. If We become aware that We cannot Process Personal Data in accordance with Your Instructions due to a legal requirement under any applicable law, We will (a) promptly notify You of that legal requirement to the extent permitted by the applicable law; and (b) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as You issue new Instructions with which We are able to comply. If this provision is invoked, We will not be liable to You under the Agreement for any failure to perform the applicable Services until such time as You issue new lawful Instructions with regard to the Processing.
- 3.3 Security. We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Annex 2 to this DPA, incorporated by reference herein (“Security Measures”). Notwithstanding any provision to the contrary, We may modify or update the Security Measures at Our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.
- 3.4 Confidentiality. We will ensure that any personnel whom We authorize to Process Personal Data on Our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.
- 3.5 Personal Data Breaches. We will notify You without undue delay after We become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by You. At Your request, We will promptly provide You with such reasonable assistance as necessary to enable You to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if You are required to do so under Data Protection Laws.
- 3.6 Deletion or Return of Personal Data. Following termination or expiration of an applicable Subscription, Supplier has no obligation to maintain or provide any related Personal Data to Client. We will delete or anonymize Personal Data collected pursuant to the Services within one (1) year after the end of the last applicable subscription. The foregoing shall apply except where We are required by applicable law to retain some or all of the Personal Data, or where We or Our Sub-processors have archived Personal Data on back-up systems, which data We and Our Sub-Processors will securely isolate and protect from any further Processing and delete in accordance with Our deletion practices for such back-up systems.
4. DATA SUBJECT REQUESTS. If a Data Subject request or other communication regarding the Processing of Personal Data under the Agreement is made directly to us, We will promptly inform You and will advise the Data Subject to submit their request to You. You will be solely responsible for (i) responding substantively to any such Data Subject Requests or communications involving Personal Data and (ii) providing Supplier Instructions with respect to such Data Subject Request.

5. SUB-PROCESSORS.



- 5.1** Agreement to Sub-Processors. You agree that We may engage Sub-Processors to Process Personal Data on Your behalf. We have currently appointed, as Sub-Processors, the Supplier Affiliates and third parties listed at <https://challengerinc.com/legal/subprocessors-list/>. We will notify You if We add or replace any Sub-Processors listed at least fifteen (15) days prior to any such changes.
- 5.2** Requirements. When We engage Sub-Processors, We will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.
- 6. DATA TRANSFERS.** You acknowledge and agree that We may access and Process Personal Data on a global basis as necessary to provide the Services in accordance with the Agreement, and in particular that Personal Data may be transferred to and Processed in the United States and to other jurisdictions where Supplier's Affiliates and Sub-Processors have operations. If Personal Data is transferred outside its country of origin, each Party and any applicable Sub-Processors of such Party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.
- 7. ADDITIONAL PROVISIONS FOR EUROPEAN DATA.**
- 7.1** Scope. This 'Additional Provisions for European Data' section shall apply only with respect to European Data.
- 7.2** Roles of the Parties. When Processing European Data in accordance with Your Instructions, the parties acknowledge and agree that You are the Controller of European Data and We are the Processor.
- 7.3** Instructions. If We believe that Your Instruction infringes European Data Protection Laws (where applicable), We will inform You without delay.
- 7.4** Objection to New Sub-Processors. We will give You the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data so long as such objection is raised within fifteen (15) days of notifying You in accordance with the 'Sub-Processors' section of this DPA. If You do notify us of such an objection, the parties will discuss Your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, We will, at Our sole discretion, either not appoint the new Sub-Processor, or permit You to suspend or terminate the affected Services without liability to either Party; provided, however, You remain liable for Fees for Services performed up to the date of Termination. The parties agree that by complying with this sub-section, Supplier fulfils its obligations under Clause 9(a) of the Standard Contractual Clauses.
- 7.5** Sub-Processor Agreements. For the purposes of Clause 9(c) of the Standard Contractual Clauses, You acknowledge that We may be restricted from disclosing Sub-Processor agreements, but We shall use reasonable efforts to require any Sub-Processor We appoint to permit it to disclose the Sub-Processor agreement to You and shall provide (on a confidential basis) all information We reasonably can.
- 7.6** Transfer Mechanisms for Data Transfers.
- (a) Supplier shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws) unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.
 - (b) You acknowledge that in connection with the performance of the Services, Supplier is a recipient of European Data in the United States. The parties acknowledge and agree to abide by and process European Data in compliance with the Standard Contractual Clauses.
 - (c) The parties agree that for the purposes of the Standard Contractual Clauses, (i) the Standard Contractual Clauses are incorporated by reference into the Agreement; (ii) Module TWO: Transfer controller to processor shall apply throughout; (iii) Supplier will be the "data importer" and Client will be the "data exporter" (on behalf of itself and Permitted Affiliates); (iv) if optional clauses are to be selected in the Standard Contractual Clauses, OPTION 2 shall apply; (v) with respect to Clause 17, the law of Ireland shall apply; (vi) with respect to Clause 18, disputes shall be resolved before the courts of Ireland; (vii) the Annexes of the Standard Contractual Clauses shall be populated with the relevant information set out in Annex 1 and Annex 2 of this DPA; (viii) execution of the Agreement evidences Client's entry into the Standard Contractual Clauses (including the information contained in Annex 1 and Annex 2 of this DPA); and (ix) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.
 - (d) To extent that and for so long as the Standard Contractual Clauses as implemented in accordance with this DPA cannot be relied on by the parties to lawfully transfer Personal Data in compliance with the UK GDPR, the applicable standard data protection clauses issued, adopted or permitted under the UK GDPR shall be incorporated by reference into the Agreement,



and the annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in Annex 1 and Annex 2 of this DPA.

- (e) If for any reason Supplier cannot comply with its obligations under the Standard Contractual Clauses or is in breach of any warranties under the Standard Contractual Clauses, and You intend to suspend the transfer of European Data to Supplier or terminate the Standard Contractual Clauses, You agree to provide us with reasonable notice to enable us to cure such non-compliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If We have not or cannot cure the non-compliance, You may suspend or terminate the affected part of the Subscription Service in accordance with the Agreement without liability to either Party (but without prejudice to any Fees You have incurred prior to such Suspension or Termination).

7.7 Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA available to You and allow for and contribute to audits, including inspections conducted by or Your auditor in order to assess compliance with this DPA. You acknowledge and agree that You will exercise Your audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section. You acknowledge that the Services are hosted by Our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that Our systems are regularly tested by independent third-party penetration testing firms. At Your written request, We will provide written responses (on a confidential basis) to all reasonable requests for information made by You necessary to confirm Our compliance with this DPA, provided that You will not exercise this right more than once per calendar year unless You have reasonable grounds to suspect non-compliance with the DPA.

8. ADDITIONAL PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION.

8.1 Scope. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

8.2 Roles of the Parties. When processing California Personal Information in accordance with Your Instructions, the parties acknowledge and agree that You are a Business and We are a Service Provider for the purposes of the CCPA.

8.3 Responsibilities. The parties agree that We will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services or as otherwise permitted by the CCPA.

9. GENERAL PROVISIONS.

9.1 Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, We reserve the right to make any updates and changes to this DPA; provided however, We agree that any such updates will not reduce substantive protections accorded to Client under this DPA without notice to Client.

9.2 Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

9.3 Limitation of Liability. Each Party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Agreement and any reference in such section to the liability of a party means aggregate liability of that Party and all of its Affiliates under the Agreement (including this DPA). For the avoidance of doubt, if a Supplier Affiliate is a party to the Agreement, the 'Limitation of Liability' section of the Agreement will apply as between Client and such Supplier Affiliate, and in such respect any references to 'Supplier', 'We', 'Us' or 'Our' will include both Supplier and any applicable Supplier Affiliate that is a Party to the Agreement. In no event shall either party's liability be limited with respect to any individual's data protection rights under this DPA (including the Standard Contractual Clauses) or otherwise.

9.4 Governing Law. This DPA will be governed by and construed in accordance with the Governing Law section of the Agreement, unless required otherwise by applicable Data Protection Laws.

9.5 Mutual indemnification. Each Party ("Indemnifying Party") shall indemnify, defend, and hold harmless the other Party, its Affiliates, and its and their officers, directors, employees, and agents (collectively, the "Indemnified Parties") from and against any and all third-party claims, losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees and court costs) arising out of or relating to: (a) a breach by the Indemnifying Party (or its personnel or subcontractors) of its obligations under this DPA, including, without limitation, any unauthorized use or disclosure of Personal Data; or (b) a violation of applicable Data Protection Laws by the Indemnifying Party, its employees, agents, or Sub-Processors (as applicable); provided that the Indemnified Party promptly notifies the Indemnifying Party in writing of the claim (provided that failure to provide such notice will not relieve the Indemnifying Party of its obligations except to the extent materially prejudiced), permits the Indemnifying Party to control the defense and settlement of the claim, and reasonably cooperates in such defense or settlement at the Indemnifying Party's expense.

10. PARTIES TO THIS DPA.

10.1 Permitted Affiliates. By signing the Agreement, Client enters into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of itself and in the name and on behalf of its Affiliates, where applicable. For the purposes of this DPA only, and except where indicated otherwise, the terms "Client", "You" and "Your" will include any of Client's Affiliates that use Services provided by Supplier.



- 10.2** Authorization. The legal entity agreeing to this DPA as Client represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Affiliates.
- 10.3** Remedies. The parties agree that (i) solely the Client entity that is the contracting party to the Agreement will exercise any right or seek any remedy any of its Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Client entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each of its Affiliate individually but in a combined manner for itself and all of its Affiliates together. The Client entity that is the contracting entity is responsible for coordinating all Instructions, authorizations and communications with Us under the DPA and will be the sole party entitled to make and receive any communications related to this DPA on behalf of its Affiliates.
- 10.4** Other rights. The parties agree that You will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on Us and our Affiliates by combining several audit requests carried out on behalf of the Client entity that is the contracting party to the Agreement and all of its Affiliates in one single audit.



Annex 1 Details of Processing

A. List of Parties

Data exporter

Name: The Client, as set forth in the Master Services Agreement (on behalf of itself and its Affiliates, as applicable)

Address: The Client's address, as set forth in an applicable Statement of Work

Contact person's name, position and contact details: The Client's contact details, as set out in the Statement of Work and/or as set out in the Client's Supplier Account.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with the Services set forth in an applicable Statement of Work

Role (controller/processor): Controller

Data importer

Name: The Richardson Company

Address: 2001 Market Street #2850, Philadelphia, PA 19103, USA

Contact person's name, position and contact details: Erin Smith, Chief Customer Officer, The Richardson 2 Commerce Square 2001 Market Street #2850, Philadelphia, PA 19103, USA

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with the Services set forth in an applicable Statement of Work

Role (controller/processor): Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred

May include the employees of the Controller or any of its Affiliates and with advance written permission of Processor, which may be withheld in Processor's reasonable discretion, certain contractors of Controller or any of its Affiliates.

Categories of Personal Data Transferred

May include usernames, passwords, names, e-mail addresses, job titles, organizational structures, IP address, responses to training modules and learning diagnostics and other information as the Controller may instruct Processor to Process (such as sales metrics, etc.) for the purpose of providing the Services described in the Agreement.

Special Categories of Personal Data

None

Frequency of the transfer

The Data Subject will interact with an online e-learning system throughout the provision of Services to Controller by Processor.

Nature of the Processing

The Personal Data may be subject to the following basic processing activities: collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, and/or erasure or destruction.

Purpose(s) of the data transfer and further processing

The provision of Services to Controller pursuant to the Agreement between Controller and Processor.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

Personal data will be retained for one year following the end of Services unless otherwise instructed by the Controller.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

The answers above also apply to (sub-) processors.

C. Competent Supervisory Authority

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Client is established in an EU Member State, the supervisory authority responsible for ensuring Client's compliance with the GDPR; (ii) where Client is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Client's representative is established; or (iii) where Client is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).



Annex 2 Security Measures

Processor has implemented the following technical and organizational measures:

- Measures to encrypt personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- 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
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing
- Measures for user identification and authorization
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for ensuring data minimization, data quality, limited data retention and erasure
- Measures for ensuring accountability

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

With respect to (sub-) processors, Processor requires the same measures as set forth above.