THIS DATA PROCESSING ADDENDUM ("**DPA**") IS ENTERED IS ENTERED BETWEEN QUALIFIED.COM, INC., A DELAWARE CORPORATION ("**QUALIFIED**"), AND THE ENTITY IDENTIFIED IN THE APPLICABLE ORDER FORM FOR THE SERVICES ("**CUSTOMER**"). THIS DPA IS AN ADDENDUM TO AND FORMS PART OF THE MAIN SERVICES AGREEMENT (OR OTHER APPLICABLE AGREEMENT) BETWEEN CUSTOMER AND QUALIFIED ("**AGREEMENT**"). THIS DPA WILL BE EFFECTIVE UPON THE PARTIES' MUTUAL EXECUTION OF AN APPLICABLE ORDER FORM.

Qualified and Customer agree as follows:

1. Definitions

For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

Controller means the entity which determines the purposes and means of the Processing of Personal Data.

Data Protection Laws means any applicable law governing the privacy or security of Personal Data Processed by Qualified in order to render Services to Customer.

Data Subject means the identified or identifiable person to whom Personal Data relates.

EEA means the European Economic Area.

European Data Protection Laws means the GDPR and other data protection laws of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

GDPR means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); (ii) the Swiss Federal Act on Data Protection and its ordinances ("Swiss FADP"), and/or (iii)the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("**UK GDPR**"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "Articles" and "Chapters" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

Personal Data means Customer Content that constitutes "personal data," "personal information," or similar information governed by Data Protection Laws that is Processed by Qualified on behalf of Customer in order to render Services to Customer.

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

Processor means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

Restricted Transfer means the disclosure, grant of access or other transfer of Personal Data to any person located in: (i) in the context of the EEA and Switzerland, any country or territory outside the EEA and Switzerland which does not benefit from an adequacy decision under the GDPR (an "**EU Restricted Transfer**"); and (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK

Government (a "**UK Restricted Transfer**"), which would be prohibited without a legal basis under Chapter V of the GDPR.

Security Incident means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Qualified or its Subprocessors.

Sensitive Data means: (a) Personal Data as defined or identified as sensitive, a special category, high risk or similar term under Data Protection Laws, including without limitation the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or GDPR; (b) Personal Data as defined under US breach notification laws, including without limitation Social Security numbers, governmental identification information, health or medical information, biometric information, and information about criminal history; and (c) Personal Data that includes any medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, health insurance information, biometric information; passwords to any online accounts, credentials to any financial accounts, tax return data, payment card information personal data of any individual who is under 16 years of age.

Standard Contractual Clauses or **SCCs** means the standard contractual clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as set out in Attachment 1.

Subprocessors means third parties that Qualified engages to Process Personal Data in relation to the Services.

Supervisory Authority: (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; (ii) in the context of Switzerland and the Swiss FADP, means the Swiss Federal Data Protection and Information Commissioner, (iii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office, and (iv) similar or equivalent regulatory bodies under respective Data Protection Laws.

UK Addendum means the International Data Transfer Addendum to the Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner's Office under S119A(1) Data Protection Act 2018 and in force as of 21 March 2022, as revised by the UK Information Commissioner's Office from time to time and as set out in Schedule 2 (UK Specific Terms).

2. Duration and Scope of DPA

(a) Scope. This DPA governs the manner in which Personal Data will be Processed. The parties agree Qualified will be the Processor and of Personal Data and Customer will be the Controller of Personal Data under this DPA and the Agreement.

(b) Details of Processing. The subject matter of Processing of Personal Data by Qualified is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the processing, the types of Personal Data and categories of Personal Data are further specified in Annex 1 of this DPA.

(c) Region Specific Terms. The Schedules to this DPA only apply if, and to the extent, region specific Data Protection Laws apply to Qualified's Processing of Personal Data.

(d) Duration. This DPA will remain in effect so long as Qualified Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

3. Customer Instructions

Qualified will Process Personal Data only in accordance with Customer's documented instructions. By entering into this DPA, Customer instructs Qualified to Process Personal Data to provide the Services and to perform its other obligations under the Agreement and any applicable Order Forms, including without limitation to (i) carry out the

Services or the business of which the Services is a part; (ii) carry out any benefits, rights and obligations relating to the Services; (iii) maintain records relating to the Service; or (iv) comply with any legal obligations relating to the Services.

4. Security

(a) Qualified Security Measures. Qualified will implement appropriate administrative, technical and physical controls designed to protect Personal Data against unauthorized access, use, acquisition, loss or disclosure (the "**Security Measures**") as described in Schedule 4 (Technical and Organizational Measures). Qualified agrees that it will maintain a SOC2/Type II certification with respect to its Security Measures. Qualified may update its Security Measures from time to time, provided the updated measures do not decrease the overall protection of Personal Data.

(b) Security Incidents. Qualified will notify Customer without undue delay after becoming aware of a Security Incident affecting Personal Data. Such notifications will describe available details of the Security Incident, including steps taken to mitigate the potential risks and steps Qualified recommends Customer take to address the Security Incident. Qualified's notification of or response to a Security Incident will not be construed as Qualified's acknowledgement of any fault or liability with respect to the Security Incident. Qualified shall not be liable or responsible for any Security Incident to the extent it arises out of any act, error or omission of Customer.

(c) Customer's Security Responsibilities and Assessment

1. **Customer's Security Responsibilities.** Customer agrees that, without limitation of Qualified's obligations under Section 4 (Security), Customer is solely responsible for its use of the Services, and (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Qualified must use or interact with to provide the Services; and (d) securing and backing up Personal Data in Customer's care, custody or control.
2. **Customer's Security Assessment.** Customer agrees that the Services, the Security Measures and Qualified's commitments under this DPA are reasonable and adequate to meet Customer's needs, including with respect to any security obligations of Customer under Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

5. Subprocessors

(a) Consent to Subprocessor Engagement. Customer acknowledges and agrees that Qualified may engage third-party Subprocessors to provide the Services. Information about currently engaged Subprocessors, including their functions and locations, is available at: http://www.qualified.com/legal/subprocessors (as may be updated by Qualified from time to time) or such other website address as Qualified may provide to customer from time to time (the "**Subprocessor Site**").

(b) Qualified Affiliate Subprocessing. Customer acknowledges and agrees that Qualified may engage its Affiliates as Subprocessors for the purposes of implementation and technical support.

(c) Requirements for Subprocessor Engagement. When engaging any Subprocessor, Qualified will enter into a written contract with such Subprocessor containing substantially similar data protection obligations no less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the

services provided by such Subprocessor. Qualified shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

(d) Opportunity to Object to Subprocessor Changes. When Qualified engages any new third-party Subprocessor after the effective date of the Agreement, Qualified will notify Customer of the engagement (including the name and location of the relevant third-party Subprocessor and the activities it will perform) by updating Subprocessor Site or providing email notice. If Customer objects to such engagement in a written notice to Qualified within 15 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and Qualified will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Service by providing written notice to Qualified only with respect to those Services which cannot be provided by Qualified without the use of the objected-to new Subprocessor.

6. Data Subject Rights

(a) Qualified's Data Subject Request Assistance. To the extent Customer, in its use of the Services, does not have the ability to address a data subject request, Qualified will (taking into account the nature of the Processing of Personal Data) provide Customer with the assistance reasonably necessary for Customer to perform its obligations under Data Protection Laws applicable to Customer to fulfill requests by data subjects to exercise their rights under such Data Protection Laws ("Data Subject Requests") with respect to Personal Data in Qualified's possession or control.

(b) Customer's Responsibility for Requests. If Qualified receives a Data Subject Request, Qualified will advise the data subject to submit the request to Customer and Customer will be responsible for responding to any such request.

7. Customer Responsibilities

(a) No Sensitive Data. Customer represents and warrants to Qualified that Customer Content does not and will not contain any Sensitive Data, and that Customer shall not provide or make any Sensitive Data available to Qualified for Processing or otherwise.

(b) Required Consents and Legal Compliance. Customer represents and warrants to Qualified that Customer has all necessary licenses, rights, disclosures, consents and permissions to collect, share and use Personal Data as contemplated in the Agreement, including without limitation such licenses, rights, disclosures, consents and permissions necessary for Qualified's Processing under the Agreement, without violation or infringement of (i) any third party intellectual property, publicity, privacy or other rights, (ii) any Data Protection Laws or (iii) any terms of service, privacy policies or other agreement. Customer agrees and consents to the disclosure of Personal Data to, or collection of Personal Data by, Subprocessors in conjunction with the Services, including without limitation IP address, cookie data, device/advertising IDs and page attribute data. Customer agrees to provide relevant individuals with a privacy policy, and disclosures required under Data Protection Laws applicable to Customer that accurately describe the Processing under the Agreement, including without limitation any cookie or tracking ID that Qualified places on Customer Properties as part of the Services, any disclosures of Personal Data to third parties, and third party use of Personal Data related to the Agreement. As between Customer and Qualified, with respect to Processing by Qualified, Customer will be solely responsible for providing the necessary notices to, obtaining the necessary clearances, consents and approvals from, and satisfying data subject requests related to, individuals with respect to the Processing contemplated under this Agreement.

(c) Children's' Personal Data. Customer agrees that its Customer Properties are not targeted to, nor does Customer knowingly collect Personal Data from, children under the age of sixteen (16).

8. Liability

The total combined liability of Qualified, whether in contract, tort or any other theory of liability, under or in connection with the Agreement and this DPA combined will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement; provided, however, that this section will not affect any party's liability to data subjects under the third party beneficiary provisions of the Standard Contractual Clauses to the extent limitation of such rights is prohibited by Data Protection Laws, where applicable.

9. Audits

(a) Customer may audit Qualified's compliance with its obligations under this Addendum up to once per year. In addition, to the extent required by Data Protection Laws, including where mandated by Customer's Supervisory Authority, Customer or Customer's Supervisory Authority may perform more frequent audits (including inspections). Qualified will contribute to such audits by providing Customer or Customer's Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services.

(b) If a third party is to conduct the audit, Qualified may object to the auditor if the auditor is, in Qualified's reasonable opinion, not suitably qualified or independent, a competitor of Qualified, or otherwise manifestly unsuitable. Such objection by Qualified will require Customer to appoint another auditor or conduct the audit itself

(c) To request an audit, Customer must submit a detailed proposed audit plan to privacy@qualified.com at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration and start date of the audit. Qualified will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Qualified's security, privacy, employment or other relevant policies). Qualified will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 9 shall require Qualified to breach any duties of confidentiality.

(d) If the requested audit scope is addressed in a SOC2 Type II, ISO, NIST or similar audit report performed by a qualified third party auditor ("Audit Reports") within twelve (12) months of Customer's audit request, and Qualified confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

(e) The audit must be conducted at a time that does not unreasonably interfere with Qualified's business activities, at the applicable facility, subject to the agreed final audit plan and Qualified's health and safety, security and other relevant policies.

(f) Customer will promptly notify Qualified of any potential non-compliance discovered during the course of an audit and provide Qualified any audit reports generated in connection with the audit, unless prohibited by European Data Protection Laws or otherwise instructed by a Supervisory Authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this Addendum. The audit reports are Confidential Information of the parties under the terms of the Agreement.

(g) Any audits are at Customer's expense. Customer shall reimburse Qualified for any time expended by Qualified or its Subprocessors in connection with any audits or inspections under this section at Qualified's then-current

professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(h) The parties agree that this section shall satisfy Qualified's obligations under the audit requirements of the Standard Contractual Clauses applied to Qualified under Clause 8.9 and to any Subprocessors under Clause 9 and Clause 13.

10. Deletion or Return of Personal Data

Qualified shall, at the expiration or termination of the Agreement, at Customer's option, delete or return all Personal Data to Customer in accordance with the procedures and timeframes specified in the Agreement, except where Qualified is required to retain copies under applicable laws.

11. Miscellaneous

(a) Conflict. Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. To the extent there is any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern.

(b) General. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that Qualified's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Qualified to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement; (b) to Qualified's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

Schedule 1 – EU Specific Terms

This Schedule 1 (EU Specific Terms) is supplemental to the DPA and sets out the terms that apply to the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer European Personal Data from Europe to Qualified or a Subprocessor in a country located outside of Europe that does not ensure an adequate level of data protection within the meaning of European Data Protection Laws.

1. Data Transfers out of the EU

(a) Data Processing Facilities. Qualified may, subject to Section 1(b) and 1(c) (Transfers out of the EEA and Transfers out of Switzerland), store and Process Personal Data in the United States or anywhere Qualified or its Subprocessors maintain facilities. Accordingly, the parties acknowledge that Customer's transmission of Personal Data to Qualified hereunder may involve a Restricted Transfer. The relevant Module(s) of the Standard Contractual Clauses that may be entered into under Section 1(b) and 1(c) (Transfers out of the EEA and Transfers out of Switzerland) of this Schedule 1 shall apply and have effect to the extent permitted and required under the EU GDPR (if and as applicable) to establish a valid basis under FADP and Chapter V of the EU GDPR 'in respect of the transfer from Customer to Qualified of Personal Data – and will not apply to the extent an alternative recognized compliance standard applies to the Restricted Transfer (e.g., binding corporate rules).

(b) Transfers out of the EEA. To the extent that any Processing of Personal Data under this DPA involves an EU Restricted Transfer from Customer to Qualified, the parties shall comply with their respective obligations set out in the Standard Contractual Clauses, which are hereby deemed entered into by the parties and incorporated by reference into this DPA.

(c) Transfers out of Switzerland. To the extent that any Processing of Personal Data under this DPA involves an EU Restricted Transfer from Customer to Qualified under the Swiss FADP, the parties shall comply with their respective obligations set out in the Standard Contractual Clauses, which are hereby deemed entered into by the parties and incorporated by reference into this DPA. General and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Swiss FADP. Accordingly, data subjects with their place of habitual residence in Switzerland may also bring legal proceedings before the competent courts in Switzerland in respect of those disputes. The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of pursuing their rights at their place of habitual residence (Switzerland).

(d) Application of updated or alternative transfer solution(s). Qualified may from time to time, vary this DPA on notice and replace the relevant set(s) Standard Contractual Clauses with:

1. any new form of the relevant Standard Contractual Clauses, the UK Addendum or any replacement therefor; or
2. another transfer mechanism, other than the Standard Contractual Clauses and/or the UK Addendum,

that enables the lawful transfer of Personal Data to Qualified under this DPA in compliance with Chapter V of the GDPR.

2. Impact Assessments and Consultations

Qualified will (taking into account the nature of the Processing and the information available to Qualified) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Qualified's information security program and the security measures applied in connection therewith; and (b) providing the other information contained in the Agreement, including this DPA.

ATTACHMENT 1 – STANDARD CONTRACTUAL CLAUSES

1. Customer will act as the data exporter and Qualified will act as the data importer.
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EU Restricted Transfer is effectuated by Customer as the data controller of the Personal Data and Qualified as the data processor of the Personal Data.
3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.
4. The certification of deletion of Personal Data as described in Clause 8(5) of the Standard Contractual Clauses shall be provided upon Customer's request.
5. Customer agrees that the provisions of Section 4(b) (Security Incidents) satisfy the requirements of the Standard Contractual Clauses between Customer and Qualified under Clause 8.6(c).
6. The audits described in Clause 8.9 of the Standard Contractual Clauses shall be performed in accordance with Section 9 of the DPA and satisfy the Parties' rights and obligations under the Standard Contractual Clauses.
7. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 5 of the DPA.
8. Customer's authorizations in Section 5 of this DPA (Subprocessors) will constitute Customer's prior written consent to the subcontracting by Qualified of the Processing of Personal Data if such consent is required under Clause 9 of the Standard Contractual Clauses.
9. Upon data exporter's request under the Standard Contractual Clauses, data importer will provide the copies of the subprocessor agreements that must be sent by the data importer to the data exporter pursuant to Clause 9(b) of the Standard Contractual Clauses, and that data importer may remove or redact all commercial information or clauses unrelated to the Standard Contractual Clauses or their equivalent beforehand.
10. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.
11. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of France.
12. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of France.
13. Annex I of the Standard Contractual Clauses shall be completed as set out in Annex 1 to this Attachment 1.
14. The Security Measures referred to in the DPA serves as Annex II of the Standard Contractual Clauses.
15. Annex III of the Standard Contractual Clauses shall be completed as set out at www.qualifed.com/legal/subprocessors.

Annex I to the Standard Contractual Clauses

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

Name: Customer as identified in the Agreement (the "data exporter")

Address: As identified in the Agreement

Contact person's name, position and contact details: As identified in the Agreement

Activities relevant to the data transferred under these Clauses: Activities relating to conversational sales and marketing platform that helps conversations with customers and prospective customers in real time using live chat, voice-calls, and chatbots as serviced by Qualified

Signature and date: these Clauses are entered into by Customer under and subject to Section 4(a) and 4(b) of Annex 1 (European Annex) to the DPA with effect from the effective date of that DPA.

Role (controller/processor): Controller or Processor

Data importer(s):

Name: Qualified.com, Inc.

Address: 50 Fremont St. Suite 300, San Francisco, CA 94105

Contact person's name, position and contact details: Lindsey Finch, DPO, privacy@salesforce.com

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature and date: these Clauses are entered into by Qualified under and subject to Section 4(a) and 4(b) of Annex 1 (European Annex) to the DPA with effect from the effective date of that DPA.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects to whom the Personal Data pertains are individuals about whom Processor Processes in connection with the Services including customers and prospective customers of Qualified's customers

Categories of personal data transferred

The categories of personal data are data provided by Customer or its End Users in connection with the Services including e-mail address and IP address.

Sensitive data transferred (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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

Categories of sensitive data

Not applicable

Additional safeguards for sensitive data

Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous

Nature of the processing

As set forth in the Agreement

Purpose(s) of the data transfer and further processing

To facilitate Qualified's provision of the Services pursuant to the Agreement.

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

The personal data will be retained for the time period needed to accomplish the purposes of processing, unless otherwise required by applicable law

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

Transfers to sub-processors are for the same purposes as transfers to the processor

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The supervisory authority of the EU Member State in which the data exporter is established. See https://edpb.europa.eu/about-edpb/about-edpb/members_en

Schedule 2 – UK Specific Terms

This Schedule 2 (UK Specific Terms) is supplemental to the DPA and sets out the terms that apply to the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer European Personal Data from the United Kingdom to Qualified or a Subprocessor in a country located outside of the United Kingdom that does not ensure an adequate level of data protection within the meaning of UK Data Protection Laws.

1. Data Transfers out of the UK. To the extent that any Processing of Personal Data under this DPA involves a UK Restricted Transfer from Customer to Qualified, the parties shall comply with their respective obligations set out in this Schedule 2 (UK Specific Terms). The clarifications made to the Standard Contractual Clauses in this DPA shall apply to this Schedule 2 (UK Specific Terms).

2. Tables

Table 1: The Parties: as stipulated in Annex 1 to the Standard Contractual Clauses**.**

Table 2: Selected SCCs, Modules and Selected Clauses: as stipulated in Attachment 1**.**

Table 3: Appendix Information: means the information which must be provided for the selected modules as set out in the Appendix of the Standard Contractual Clauses (other than the Parties), and which for this Schedule 2 is set out in Attachment 1.

3. Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Schedule 3 – US Specific Terms

This Schedule 3 (US Specific Terms) is supplemental to the DPA and sets out the terms that apply to the extent Customer's use of the Services requires Processing of United States Personal Data.

1. Definitions

CCPA means the California Consumer Privacy Act of 2018, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

US Data Protection Laws means all state and federal data privacy regulations of the United States of America applicable to Qualified's Processing of Personal Data under the Agreement, including the CCPA.

The terms "business," "business purpose," "commercial purpose," "sell," "sharing," and "service provider" shall have the respective meanings given thereto in the CCPA, and "personal information" shall mean Personal Data that constitutes personal information governed by the CCPA.

2. It is the parties' intent that with respect to any personal information, Qualified is a service provider. Qualified shall not (a) sell or "share" any personal information; (b) retain, use or disclose personal information for any purpose other than for the specific purpose of providing the Service or to perform a business purpose; (c) retain, use or disclose the personal information for a commercial purpose outside of the direct business relationship between Qualified and Customer; or (d) combine personal information with other person information that it receives from other sources, including its own interactions with a consumer, provided that Qualified may combine personal information if it is within the scope of the Services provided to Customer as permitted under the CCPA. The Customer shall have the right, upon written notice to Qualified, to take reasonable and appropriate steps set forth in the Agreement to stop and remediate any unauthorized use of personal information. Qualified will notify the Customer if Qualified makes a determination that it can no longer meet its obligations under the CCPA.

3. Customer provides personal information to Qualified for the limited and specified purposes of facilitating Qualified's provision of the Services as a service provider. The parties acknowledge that Qualified's retention, use and disclosure of personal information authorized by Customer's instructions stated in the DPA are integral to Qualified's provision of the Services and the business relationship between the parties.

Schedule 4 -Technical and Organizational Measures

1. **Security Staffing and Background Checks.** Organizational management and dedicated staff responsible for the development, implementation and maintenance of Qualified's information security program. Employees are subject to background checks prior to employment. Employees must complete management-approved security training during onboarding and revisit such training annually throughout their tenure.
2. **Audit and Risk Assessment.** Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Qualified's organization, monitoring and maintaining compliance with Qualified's policies and procedures, and reporting the condition of Qualified's information security and compliance to internal management.
3. **Security Controls** Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).
4. **Access Controls.** Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (*e.g.* use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
5. **Password Security.** Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Qualified's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Qualified's computer systems, and (v) newly issued passwords must be changed after first use.
6. **System Event Logging.** System audit or event logging and related monitoring procedures to proactively record user access and system activity.
7. **Physical Security.** Physical and environmental security of areas containing Personal Data managed by Qualified that are designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Qualified's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
8. **Operational Procedures.** Operational procedures and controls designed to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media designed to render data contained therein as undecipherable or unrecoverable prior to final disposal or release from Qualified's possession.
9. **Change Management.** Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Qualified's technology and information assets.
10. **Incident response.** Incident response management procedures designed to allow Qualified to investigate, respond to, mitigate and notify of events related to Qualified's technology and information assets.
11. **Network Security.** Network security controls that utilize firewalls and segregated access, and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
12. **Vulnerability Management Processes.** Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code. Third party vulnerability assessments are conducted periodically and vulnerabilities are remediated as appropriate in accordance with Qualified's internal risk assessment policies.
13. **Business Continuity/Disaster Recovery.** Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters. Qualified Business Continuity and Disaster Recovery procedures (including restoration from backups) are reviewed and tested annually.
14. **Policy Review.** Qualified's security and privacy policies are reviewed and approved annually for Qualified's business operations.