DATA SECURITY AND DATA PRIVACY ADDENDUM

THIS DATA SECURITY AND DATA PRIVACY ADDENDUM (the “Addendum”), as amended from time to time by Web.com Group, Inc., a Delaware corporation, its subsidiaries, affiliates, predecessors, successors and assigns (the terms “Web.com,” “us,” “we” and/or “our” shall refer to Web.com), between you (the terms “Customer,” “you” and/or “your” shall refer to the individual, entity or organization that accepts this Agreement, has access to your account or uses the Services) and Web.com, sets forth the terms and conditions applicable to your purchase and/or use of our products and services (collectively, the "Services") as further set forth herein. You and Web.com together may be referred to herein as the “Parties” and each may be referred to herein as a “Party.” This Agreement explains our obligations to you, and your obligations to us in relation to any Services you purchase or otherwise utilize.

This Addendum is an integral part and is an amendment to the agreement(s) currently in place (“Agreement”) between you and Web.com. The terms of both the Data Security Schedule and the Data Privacy Schedule establish requirements in connection with Company’s performance of the Services, including without limitation security and privacy requirements that protect Web.com Information Assets and Non-Public Information (as defined below).

1. Definitions.

    a. “Applicable Laws” includes without limitation Security Laws (as defined herein), in U.S. or foreign jurisdictions, in which Services are performed or whose residents are Data Subjects Personal Information Processed by Company during its performance of Services under the Agreement (“Services”).

    b. “Breach” means the acquisition, access, use, or disclosure of Non-Public Information in a manner that violates the privacy or security requirements in the Agreement and compromises the security of Non-Public Information or privacy of Personal Information.

    c. “Customer Information” means any information belonging to Customer.

    d. “Information Assets” means, collectively, information in the possession, custody, or control of Web.com or its Affiliates and the administrative, physical, and technical infrastructure and resources that support Processing such information.

    e. “Non-Public Information” includes but is not limited to:

        i) Internal Web.com information, which means non-sensitive Web.com information shared and distributed broadly within Web.com, but which Web.com seeks to limit to distribution only within its organization;

        ii) Customer Information, which may include Web.com Personal Information and credit card details;

        iii) Any other Web.com Personal Information, including without limitation Web.com Personal Information relating to Web.com employees or other members of Web.com’s workforce;

        iv) Personal Information relating to workforce members of Web.com Customers; and

        v) Any other Confidential means, including without limitation:

            (1) Trade secrets, hardware and software designs and code, schematics, drawings, and product or service specifications and documentation;

(2) Business and product plans, budgets, financial records, forecasts, information about potential customers or vendors, customer or vendor lists, and other financial and sales information;

(3) Information received from third parties and treated as confidential information under nondisclosure agreements with such third parties;

(4) Human resources information about workers, including without limitation compensation information, employment reviews, contact information, and disciplinary information;

(5) Information relating to Web.com's security posture, which could, if compromised, harm the security of the Information Assets, including without limitation details about Web.com's security controls and safeguards, passwords, and private encryption keys; and

(6) Other confidential business information.

f. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Non-Public Information or interference with system operations in an information system used for Processing Non-Public Information.

g. "Security Laws" means all international, foreign, federal, state, provincial, and local laws, executive orders, rules, regulations, ordinances, codes, orders, and decrees of all governments or agencies of any U.S. or foreign jurisdictions relating to the security of Personal Information or Information Assets, including but not limited to requirements for protecting the confidentiality, integrity, and availability of Personal Information; requirements to implement administrative, physical, and technical safeguards against reasonably anticipated threats or hazards to the security or integrity of Personal Information and unauthorized uses or disclosures of Personal Information; breach notification requirements; and similar governance requirements for safeguarding Personal Information.

h. "Subcontractor" means a third party with which Company contracts with (upon prior written approval from Web.com), in order to accomplish work or services contemplated under the Agreement referenced herein.

i. "Web.com Security Requirements" means the document attached hereto as Attachment 1 and incorporated by reference herein, which sets forth minimum security requirements that Company must meet as a condition of performing critical information technology Services for Web.com, including but not limited to Services involving access to or Processing of Non-Public Information and access to Web.com's Information Assets.

2. Security Obligations. In delivering the Services to Web.com, Company will maintain reasonable and appropriate administrative, technical, and physical safeguards to:

a. Ensure the integrity and confidentiality of Non-Public Information stored within, or transmitted to or from, the Information Assets;

b. Protect against any reasonably anticipated (i) threat or hazards to the security or integrity of the Non-Public Information, Information Assets, or the Services, and (ii) unauthorized uses or disclosures of the Non-Public Information, Information Assets, or the Services; and

c. Ensure compliance with applicable Security Laws by Company's officers, employees, contractors, Subcontractors, and agents.

3. Web.com Security Requirements. Without limiting the generality of Section 2 above, Company shall maintain a written information security program that complies with this Addendum, all applicable Security Laws as well as the Web.com Security Requirements in order to secure Company's delivery of Services, (b) Company's Processing of Non-Public Information, and (c) Company's access to and use of Information Assets.

4. Security Incidents and Breaches.

    a. Company shall inform Web.com of Security Incidents or Breaches in accordance with the notification requirements in the Web.com Security Requirements. Company shall also mitigate the harmful effects of Security Incidents or Breaches in accordance with the Web.com Security Requirements.

    b. Company shall, at its sole expense, make any notifications of a Breach to the persons or media outlets, at the time, and in the manner it is required to do so under applicable Security Laws. Company shall notify Web.com of any request by a law enforcement official or agency to delay breach notification and provide Web.com a copy of the request in writing. Company shall comply with all applicable requirements under Security Laws for the content of such notifications. Company shall obtain Web.com's approval of the content of any breach notification before sending it, which approval shall not be unreasonably withheld.

    c. Company shall provide reasonable cooperation and information reasonably requested by Web.com:

        i) To facilitate Web.com's conducting and documentation of an assessment of the security risks arising from or associated with a Security Incident or Breach;

        ii) To facilitate compliance with Web.com's notification obligations if Web.com informs Company that it has its own requirement(s) under applicable Security Laws to provide notifications of a Breach; and

        iii) To facilitate and implement technical solutions that may be needed to detect and eliminate the security incident

    d. Company shall promptly, upon delivery of an itemized statement, reimburse Web.com for any and all expenses incurred by Web.com in connection with responding to or making a notification of a Security Incident or Breach caused by the acts or omissions of Company or any of its officers, employees, contractors, Subcontractors, or agents. Such expenses shall include, without limitation:

        i) A charge for the time of Web.com employees and contractors spent in responding to the Security Incident or Breach, charged at a commercially reasonable hourly rate;

        ii) Mailing costs, reasonable attorneys' fees, credit monitoring costs, and fees and expenses paid to communications consultants, and computer forensic and other investigators;

        iii) Any fine(s) incurred by Web.com imposed by any governmental agency, financial institution or court system resulting from the aforementioned Security Incident or Breach notifications; and

        iv) Any additional financial impacts including but not limited to customer retention and general business impacts.

5. Additional Security-Related Requirements.

a. "Security Instructions" means any of Web.com's security-related instructions to Company hereunder, including without limitation general instructions in the Web.com Security Requirements or other portions of the Agreement or specific instructions provided to Company in connection with Company's performing the Services. Company will Process Non-Public Information in accordance with Web.com's reasonable Security Instructions and applicable Security Laws.

b. Company shall promptly notify Web.com if:

   i) Company believes that any Security Instructions violate Applicable Laws; or

   ii) Company is or may be unable to comply with any Security Instructions for any reason, including without limitation due to other requirements, applicable limitations, or changes in Applicable Laws.

c. The parties shall negotiate any changes in Security Instructions in good faith to address Applicable Laws, other requirements, or applicable limitations.

d. Company shall ensure that any Subcontractor receiving or Processing Non-Public Information from or on behalf of Company, agree to the same security restrictions and conditions that apply to Company with respect to such Non-Public Information, including without limitation by entering into a written agreement with such Subcontractor that establishes security and Security Incident/Breach notification terms and requirements that are substantially the same in form and substance as the terms and requirements in this Addendum, including without limitation the requirements of the Web.com Security Requirements and, to the extent Subcontractors are processing Web.com Personal Information in a location that is not an Approved Third Country, and such Subcontractor is not Privacy Shield certified, the EU Standard Contractual Clauses.

e. Company shall be fully responsible for the acts and omissions of its employees as well as for the acts and omissions of any Subcontractors retained to provide all or a portion of the Services and remains fully liable for the acts or omissions of Subcontractors giving rise to a breach of any provision of this Addendum or any other provision of the Agreement, to a Security Incident, or to a Breach as if they were Company's own acts or omissions.

f. Upon Web.com's request, Company shall provide Web.com with such reasonable information that Web.com, a Web.com customer, or governmental entity may request from time to time to evidence the compliance of Company, a Subcontractor, or other agent of Company with this Addendum or applicable Security Law.

6. Company Compliance with Applicable Laws and Regulations.

a. Company shall at all times comply with applicable obligations under (i) Security Laws or Regulations that apply to the Information Assets or Non-Public Information, (ii) Security Laws to which Company is subject as a service provider having access to the Information Assets or Processing Non-Public Information or Processor of Web.com Personal Information (including without limitation any Special Categories of Data), or (iii) Security Laws that are otherwise applicable to Company's security practices in connection with the Services.

b. Company shall not knowingly perform Services or the Agreement in such a way as to cause Web.com to violate any requirement under applicable Security Laws.

c. Company shall promptly cooperate with and provide Web.com with the assistance Web.com deems necessary to ensure Non-Public Information is Processed as part of Company's Services in compliance with applicable Security Laws.

d. To the extent Company creates, receives, maintains, or transmits Web.com Personal Information of members of the workforce of Web.com as a result of the providing the Services (including without limitation any Special Categories of Data), and Processes that Web.com Personal Information as a Controller, Company shall at all times comply with its obligations under applicable Security Laws as a Controller in relation to such Personal Information.

7. Termination Right. Notwithstanding anything to the contrary in the Agreement, Web.com shall be entitled to terminate this Agreement immediately upon written notice to Company, without a cure period, in the event of a breach, default, or failure to comply with term or provision of this Addendum or the Web.com Security Requirements.

8. Company Insurance. Company shall maintain appropriate Privacy/Cyber/Network Security /Professional Liability coverage in the amount of not less than $1,000,000 per incident and $4,000,000 in the aggregate with coverage to specifically provide protection against liability for the following: (a) privacy breaches and resulting liability arising from the loss or disclosure of Web.com Data or Personal Information; (b) denial or loss of service; (c) introduction, implantation or spread of Malicious Software; and (d) unauthorized access to or use of computer systems to include first party coverage for forensic investigation, notification and credit monitoring and third party coverage for network security errors and omissions with no exclusions for unencrypted portable devices or media or cyber events. Company shall maintain such insurance for at least a two (2) year period from the termination of this Agreement and any Continuation Period, and during this two (2) year period Company shall use its best efforts to ensure that there is no change of the retroactive date on all such insurance coverage. No changes are to be made to these specifications without prior written specific approval by the Web.com.

SCHEDULE 1
SECURITY REQUIREMENTS

1. In general and always applicable

General clauses

a. Company shall comply, and shall ensure that the Company's personnel and Subcontractors' personnel comply with the Security Clauses in this document at all times when performing the Services.
b. Company shall promptly provide Web.com with any documentation, information, certifications or declarations requested by Web.com which is in Company's, or its Subcontractors' possession or under Company's or its Subcontractors' control for the purpose of demonstrating Company's compliance with the Security Clauses in this document.
c. Company shall comply, and shall ensure that the Company personnel and its Subcontractors' personnel comply with the Web.com Policies located at (https://legal.web.com/) and Standards and any other documents attached to these Security Clauses (called "Web.com Policies") and which may be amended from time to time.
d. Company and any Subcontractors or third party involved in providing the Services are entirely responsible for providing the appropriate security measures to ensure protection of their own private internal network and information whether it is connected to the Web.com network or not.
e. Company agrees that all data and information connected with the Services must be exportable to Web.com in a secure manner on request from Web.com.
f. Company agrees that at Web.com's request, all data and information connected with the Services must be returned to Web.com within 21 days from the termination date of the Agreement by way of two separate and secure copies. After confirmation of successful transfer, all Web.com data must be securely removed from all Company's infrastructure.
g. Company agrees that upon termination of the Agreement and with permission of Web.com it shall erase, destroy and render unrecoverable all Web.com data and certify in writing that these actions have been performed.

2. Hosting, operations or the provision of cloud

Data handling

a. Company shall ensure the service infrastructure guarantees the integrity, availability and confidentiality of Web.com assets, including all data, information and intellectual property rights.
b. Company shall manage Web.com information and data ensuring it has the appropriate level of privacy and protection in line with international ISO 2700x security standards and any other governing security standards and applicable laws at all times.
c. Company shall take all commercially reasonable efforts, including technical and organizational measures, to secure Web.com's data from loss, leakage, disclosure, unauthorized or improper access, use, change, or destruction. Company shall be required to document and present to Web.com such technical and organizational measures as well as any incidents of data loss, leakage, disclosure, or unauthorized or improper access, use, change or destruction in a prompt manner or upon request.

Service security

a. Company shall notify Web.com promptly, but no more than thirty (30) days, of any changes to the Services or the agreed service infrastructure being made which could minimize the security posture from the initial start time of the Agreement.

Reports

a. Company shall periodically (at least once per year) deliver the ISAE3402 or comparative reports (for example SSAE16 SOC II), the Payment Card Industry (PCI) Attestation of Compliance, as well as any additional relevant to the Services to Web.com throughout the period of the Agreement.
b. Company shall ensure other service certifications if available such as ISO 2700x, penetration test results or other valid reports will be provided to Web.com.

Right to audit

a. Company grants to Web.com and any internal or external auditors ("Auditor") assigned by Web.com, a right of access to Company facilities and any other sites from which Company (including any Subcontractors) performs the Services up to a maximum of twice per year.
b. Company shall ensure that Company and any personnel from its Subcontractors provide all necessary assistance to and co-operate with the Auditor including providing evidence of controls in place and functioning properly, access to and logs from the systems, documents and any other relevant service information.
c. Web.com shall:
    i) give Company five (5) business days written notice of when an audit will be conducted and an estimation of the scope, duration and effort of the audit; and
    ii) state the purposes of the audit.
d. IT Audits may pertain to any of the following:
    i) Verification that the Services are being provided in accordance with these Security Clauses and the applicable laws, and/or
    ii) Internal and external penetration tests of the infrastructure or applications hosted (ethical hacking).
e. Company shall solve all issues unveiled during the IT audits to Web.com's satisfaction in a timely manner, but no later than fifteen (15) business days.
f. Company may provide Web.com a generic ISAE 3402 or equivalent report issued by a reputable firm. In the event that Web.com determines that such a report is insufficient, incomplete or its scope is not broad enough for Web.com's auditing or controlling purposes, Web.com may either:
    i) Request a customized ISAE 3402 or equivalent report at Web.com cost, or
    ii) Perform the audits as defined in this clause.

Network and cloud security documentation

a. Company shall prepare and submit to Web.com on request an architecture and configuration document applicable to the Services indicating where Web.com data is stored and how the Services are securely provided and configured, their essential characteristics, service and deployment models.

Encryption

a. Company agrees that they will not utilize any "home-grown" or internally developed encryption methods to protect Web.com systems, the Services or data.
b. Encryption algorithms strength must be as high as possible in compliance with known best practice encryption requirements and applicable laws.
c. Company agrees that the following must be strongly encrypted:
    i) Data at rest, in storage, in backup or disaster recovery repositories;
    ii) Data or communications traffic in transit between servers, databases, data repositories and client systems;
    iii) Any media leaving Company's facilities;

iv) Any mobile and portable devices used in provision of the Services; and
v) Monitoring and audit logs provided to Web.com.

Risk management

a. Company shall have and must use appropriate risk review and testing procedures in connection with the Services provided, based as a minimum on information usage, access controls, security controls and location(s).
b. A risk management process must be conducted at least once a year and the scope and results shared with Web.com on request.

Continuity service

a. Company agrees to maintain emergency and contingency plans for the facilities in which information systems that process Web.com data are located.
b. Company agrees to maintain redundant storage and its procedures for recovering data must be designed to reconstruct Web.com data in its original or last-replicated state from before the time it was lost or destroyed.
c. Retention periods and deletion of data for backups or redundant storage must be in line with applicable laws regarding the data or information type. Company further agrees that data shall not be retained any longer than necessary, according to applicable law, if no longer in use.

Separation of functions, roles and responsibilities

a. Company agrees that in accordance with Web.com requirements, duties and areas of responsibility are defined and are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Services, Web.com's assets, service infrastructure, information, data, applications, functions or processes.

Capacity and outage planning

a. Company agrees to deliver the agreed operational service performance, availability and user base coverage for the entire Agreement term.
b. Company agrees that all planned service outages or updates which will or can be foreseen to cause an interruption to the agreed Services, its infrastructure, operations, applications, functions, processes or data will require Company to inform Web.com as soon as possible in advance and by no less than ten (10) business.
c. All planned outages must be made out of regional working hours.

Security activities

d. Company agrees to provide a reliable service fit for purpose and whose infrastructure is updated with all current vendor patches, protected against malware, virus, denial of service or hacking attempts and is suitably protected providing a private and controlled deployment model.
e. Company maintains up to date security documents describing its security measures and the relevant service procedures which must be provided to Web.com on request.

Data communications

a. Company agrees that all data communication between Web.com's infrastructure and Company service infrastructure must first be approved by Web.com, before any data transmission effectively occurs.

b. When the Agreement is terminated for whatever reason or becomes expired, all access methods must be revoked and Company will not be further authorized to use the communication channel(s) or Services.

Access to Web.com assets

a. Company agrees that only personnel involved in provision of the Services on a least privilege basis, may access data contained within the Web.com service infrastructure and that they are subject to the Company's confidentiality obligations. The Parties agree that Web.com may require such personnel to participate in certain training upon request.
b. Company agrees that they will maintain and update a record of personnel authorized to have access Web.com infrastructure or data and identify those personnel who may grant, alter or cancel authorized access to data and resources.
c. Company agrees to store passwords in a way that makes them unintelligible while they are used.
d. Company agrees where authentication mechanisms are based on passwords, that they are renewed at least every ninety (90) days, are at least eight characters long and are complex, and restrict user from reusing the previous ten (10) passwords.
e. Company monitors, or enables Web.com to monitor, repeated attempts to gain access to the information system using an invalid password.
f. Company agrees that access rights are removed as soon as possible upon (a) completion of Services; (b) termination of agreement; (c) or within a period thirty (30) days of inactivity.
g. Company shall review their personnel's access to Web.com's assets or data quarterly and promptly remediate any discrepancies and provide a report to Web.com in writing.
h. Upon Web.com's request the Company will disclose the results of the last access review and the remediation actions.
i. Shared access credentials are forbidden and each access to the Web.com service infrastructure must be personally identifiable.

Separation of environments

a. Company agrees that the development, test, UAT, training, integration, operational or production environments must be separated to ensure that data cannot be leaked between them or other Company customers or networks.
b. Company agrees that Web.com production data must never be migrated or used outside of the production area without first being fully depersonalized or anonymized.
c. Company shall comply with best practices in that a proper change management process (containing at a minimum planning, authorization, testing, documentation, change and deployment) is documented and followed when transferring any software from a non-productive to the production environment.

Host/servers security

a. Company agrees to maintain an inventory of all hosts/servers and media on which Web.com data is stored. Access to these inventories is restricted to personnel authorized in writing by the Company to have such access.
b. Company shall disclose their processes to Web.com for monitoring the integrity and availability of these hosts/servers on request.
c. When the Agreement is terminated for any reason or becomes expired the Company shall revoke all access to Web.com data and Company personnel will not be further authorized to access Web.com assets involved in the Services.
d. Company shall perform periodic scans of the network perimeter and key network / domain components to ensure vulnerabilities are identified. Remediation should occur according to a risk-based methodology.

Physical security at Company facilities

a. Company agrees that it limits access to facilities where information systems that process Web.com data are located in a physically secure facility or facilities and access to these facilities is granted only to identified and authorized individuals.
b. All physical security controls and the process for entry must be regularly checked, tested and documented by Company and if required by Web.com the results shared.
c. Company agrees that its physical facilities use industry standard systems to protect against loss of data, due to power supply failure or physical damage due to natural disasters.
d. Company agrees to maintain records of the incoming and outgoing media containing Web.com data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of data they contain.
e. Company agrees to use industry standard best processes to delete Web.com data when it is no longer needed and will provide a certificate of destruction upon Web.com's request for both physical and electronic records.

Incident management

a. Company agrees that an escalation procedure must be in place, which will include, managing any service operation or security issues, incidents, unlawful access or breaches, loss, disclosure or alteration of data and their monitoring, resolution and notification to Web.com responsible persons immediately upon knowledge but not to exceed twenty four (24) hours.
b. Company agrees that the incident management procedure will include the notification to Web.com, an investigation of the incident(s), provision of detailed information about the incident and the steps taken to mitigate the effects and to minimize any damage resulting from the incident.
c. Company agrees that the information in the previous clause must allow Web.com to be in a position to track disclosures of Web.com data, including what data has been disclosed, to whom and when.
d. Company agrees that they will provide Web.com with a single point of contact (or group appointed as security officers responsible for coordinating and monitoring the security rules and procedures) for all security related questions and communications for any security related events or incidents throughout the duration of the Agreement.

Feature disabling capabilities

a. Company agrees that within a 24-hour time period they will either:

    i) disable all or part of the Services, or
    ii) disable access to all or part of the Services

    when informed to do so by Web.com if a security issue is identified by Web.com which is or may affect the integrity, confidentiality or operation of the Services.
b. Company shall provide Web.com with this feature or a total shutdown capability within the defined timeframe and a documented process to invoke it.
c. The total or partial Services shutdown capability must be invoked in case of an attack, data compromise or data theft where no other option to prevent it is immediately available.

Monitoring and reporting

a. Company agrees that they log, access and use of information systems containing Web.com data, registering the access (user) ID, IP, time, authorization granted or denied, and relevant activities performed and that these logs are available to Web.com in a secure and protected manner. Company further agrees that all log times are properly synchronized with a single reference time source and time zone, such as an NTP and GMT, respectively.

b. Company agrees that controls are in place to monitor and prevent individuals assuming any access rights they have not been assigned, to gain access to the agreed Services or Web.com data.
c. Company shall provide Web.com with information about its log review policy and procedures on request.
d. Logs with any security relevant events have to be retained for an appropriate period of time up to a minimum of twelve (12) months and must contain sufficient information to establish what events occurred and the event sources or origins.

Deletion or change in service functionality

a. Company agrees that if the agreed service functionality is deleted or changed so that it no longer performs in the same manner as that which was offered at the time the Agreement was entered into, the Company must inform Web.com as soon as possible or at least in advance by six (6) months before any change(s) actually takes place.
(Note: This notice period is required by Web.com to make the required changes to the service offering and any documentation. To implement such changes, the notice from Company in regard of such functionality changes must provide detailed information on the affected functionality itself, the replacement or alternative to be provided, how this can be tested before implementation or if this is not the case how Web.com might fulfil the original functionality in another way.)
b. Company agrees that if the agreed service functionality is expanded so that new data communication or storage takes place in different geographical regions or with new suppliers as that which was offered at the time the Agreement was entered into, the Company must inform Web.com as soon as possible or at least in advance by six (6) months before any change(s) actually takes place.

Application security

a. Company agrees at all times to provide and maintain its Services and any provided application software are and remain secure from those vulnerabilities as described in either:

i) The Open Web Application Security Project's OWASP Top Ten Project (http://www.owasp.org), or
ii) The CWE Top 25 programming errors (http://cwe.mitre.org/top25/), or
iii) The SANS top 25 software errors (http://www.sans.org/top25-software-errors/).

b. Company agrees that applications made available to Web.com must include security test, at least annually, and that these test results, scope and any mitigations made, are available to Web.com on request and immediately following any major changes. Remediation should occur according to a risk-based methodology.

SCHEDULE 2
PRIVACY REQUIREMENTS

1. Definitions.

a. “Adequate Level of Protection” means adequate protection for Personal Information in force in a nation, as determined by the European Commission.

b. “Affiliate” means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with such party, where “control” means the possession, directly or indirectly, of the power to direct, or cause the direction of the management and policies of such person, whether through the ownership of voting securities, by contract or otherwise.

c. “Applicable Laws” has the meaning ascribed to it in Section n of the Agreement and includes without limitation Privacy Laws in U.S. or foreign jurisdictions in which Services are performed or whose residents are Data Subjects of Personal Information Processed by Company during its performance of Services under the Agreement.

d. “Approved Third Country” means any member of the EEA or any other country that the European Commission has determined has an Adequate Level of Protection.

e. “Controller” means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Information; where the purposes and means of Processing are determined by applicable Privacy Laws, the Controller or the specific criteria for the Controller's nomination may be designated by applicable Privacy Laws.

f. “Data Exporter” has the meaning ascribed it in Clause 1(b) of the EU Standard Contractual Clauses.

g. “Data Importer” has the meaning ascribed it in Clause 1(c) of the EU Standard Contractual Clauses.

h. “Data Subject” means an identified or identifiable living natural person, including but not limited to a member of the workforce of a Web.com customer, job candidates, or a member of Web.com’s workforce.

i. “EEA” means the collection of nations known as the European Economic Area.

j. “EEA Personal Information” means Personal Information that is stored, is maintained, or otherwise originates from a member state of the EEA.

k. “EU Standard Contractual Clauses” means the model contractual clauses governing data protection for the transfer of Personal Information to Processors established in countries that do not ensure an Adequate Level of Protection pursuant to European Commission Decision C(2010)593.

l. “Personal Information” means:

i) Any information maintained about a Data Subject, including (1) any information that can be used to distinguish or trace a Data Subject’s identity, such as name, social security number,

date and place of birth, mother's maiden name, geo-location, or biometric records; and (2) any other information that is linked or linkable to a Data Subject, such as medical, educational, financial, and employment information;

ii) Any information relating to an identified or identifiable living natural person; or

iii) Any information defined as "personal information," "personally identifiable information," "personal data," or similar expressions under applicable Privacy Laws.

m. "Privacy Authority" means a supervisory authority with responsibility for privacy or data protection matters in a given jurisdiction.

n. "Privacy Laws" means all applicable foreign, federal, state, and local laws, executive orders, rules, regulations, ordinances, codes, orders, and decrees of all governments or agencies of any jurisdiction relating to the privacy of Personal Information, including but not limited to requirements for providing notification to Data Subjects about the collection, use, sharing, or disclosure of Personal Information; providing choices to such Data Subjects about the collection, use, or disclosure of Personal Information; limiting the onward transfer of collected Personal Information; providing Data Subjects access to Personal Information collected about them to afford them the ability to correct, amend, or delete that Personal Information; safeguarding that Personal Information to protect it from loss, misuse, or unauthorized access, disclosure, alteration, or destruction; taking steps to make sure Personal Information continues to be accurate, complete, current, and reliable for its intended use; establishing mechanisms to investigate privacy complaints or resolve disputes about the handling of Personal Information; and similar Personal Information governance requirements.

o. The terms "Process," "Processing," and "Processed" mean any operation or set of operations which is performed upon Personal Information whether or not by automatic means, including, but not limited to, creating, receiving, accessing, collecting, recording, organization, retaining, storing, maintaining, adapting or altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, blocking, erasing and destroying Personal Information and any equivalent definitions in applicable Privacy Law to the extent that such definitions should exceed this definition in scope.

p. "Privacy Authority" means a supervisory authority with responsibility for privacy or data protection compliance in the jurisdiction in which a member of the Web.com Group is established or a jurisdiction in which a member of the Web.com Group is acting as a Data Exporter by transmitting Web.com Personal Data to Company.

q. "Processor" means a natural or legal person, public authority, agency, or any other body which processes Personal Information on behalf of the Controller.

r. "Special Categories of Data" means Web.com Personal Information that contains a Data Subject's social security number, driver's license number, government-issued identification card number, financial account or payment card number, code or password that would permit access to a financial account, mother's maiden name, biometric information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life.

s. "Web.com" means Web.com and its Affiliates.

t. "Web.com Personal Information" means Personal Information received from or created on behalf of Web.com, which Company Processes in connection with providing the Services, including but not limited to Personal Information about members of the workforce of a Web.com customer, partner or client as well as job candidates or members of Web.com's own workforce.

2. Processing of Web.com Personal Information. The parties acknowledge that Company will have access to Web.com Personal Information in performing the Services under the Agreement, and, as part of the Services, Company shall Process Web.com Personal Information in accordance with this Section.

   a. Web.com hereby appoints Company as a Processor in respect of all Web.com Personal Information Processed by it in order to provide the Services.
   b. Company will Process Web.com Personal Information to the extent and in a manner necessary to provide the Services and in accordance with Web.com's instructions (which may be specific or general in nature as set out in the Agreement or as otherwise as Web.com may direct Company when it is performing the Agreement), and shall not Process Web.com Personal Information for any other purpose.
   c. Company is permitted to make the following disclosures or other onward transfers ("Disclose" or "disclosures") of Web.com Personal Information:

      i) As permitted or required by the Agreement to deliver the Services;

      ii) disclosures to Subcontractors and other agents subject to Section 2(h) below; and

      iii) disclosures permitted under the Confidentially Section(s) of the Agreement.

   d. Company acknowledges that it has reviewed Web.com's Privacy Policy (located at https://assets.web.com/legal/English/PrivacyPolicy.pdf) ("Policy"), which is incorporated by reference herein. Company further acknowledges that it has read and understood the Policy and will use its best efforts to facilitate its and Web.com's compliance with the Policy to the extent the Policy applies to the Services and Company's conduct. Company represents and warrants that its acts and omissions during the performance of the Agreement shall not cause Web.com to be in violation of the Policy. Web.com shall be entitled to amend the Policy from time to time by posting a new version to Web.com's website at https://legal.web.com/ (or such successor site as designated by Web.com). Web.com may, but shall have no obligation to, notify Company of material changes to the Policy. Notwithstanding the foregoing, Company is responsible for checking Web.com's website for amendments to the Policy and will at all times be subject, under the foregoing provisions of this Section, to the then-current version of the Policy.

   e. Company shall promptly notify Web.com if:
      i) Company believes that any of Web.com's privacy-related instructions hereunder regarding Web.com Personal Information violate Applicable Laws; or
      ii) Company is or may be unable to comply with Web.com's privacy-related instructions hereunder or any provisions of the Agreement, including the Policy, for any reason, including but not limited to requirements, limitations, or changes in Applicable Laws.

   f. Company acknowledges that Web.com owns all right, title, or interest (including without limitation any intellectual property rights in Web.com Personal Information and Company has no such ownership.
   g. Company shall limit the disclosure of Web.com Personal Information in accordance with Confidentiality terms of the Agreement and applicable law. In making any such disclosure, Company shall use its best efforts to disclose only the minimum amount of Web.com Personal Information reasonably necessary to accomplish the intended purpose of the disclosure.
   h. Company shall ensure that any Subcontractor or other agent receiving or Processing Web.com Personal Information from or on behalf of Company, agree to the same restrictions and conditions that apply to Company with respect to such Web.com Personal Information, including without limitation by entering into a written agreement with such Subcontractor or other agent that establishes privacy terms and requirements that are substantially the same in form and substance as the terms and requirements in this Addendum, which will include without limitation, if necessary, EU Standard Contractual Clauses to govern any transfer of Web.com Personal Information to a location that is not an Approved Third Country.

i. Company shall be fully responsible for the acts and omissions of Company's employees as well as the acts and omissions of Subcontractors retained to provide all or a portion of the Services. Company remains fully liable for the acts or omissions of Subcontractors or other agents giving rise to a breach of any provision of this Addendum or any other provision of the Agreement as if they were Company's own acts or omissions.
j. In connection with delivering Services, Processing Web.com Personal Information, or the use of Subcontractors or other agents under subsection (h), Company shall not, and shall not permit a Subcontractor or other agent to, export any Web.com Personal Information outside the United States without Web.com's advance written consent under Section 7(a) below.
k. Company shall not sell, license, rent, or lease Web.com Personal Information to third parties.
l. If Company is a "Business Associate" within the meaning of Health Insurance Portability and Accountability Act of 1996, Public Law Number 104-191 ("HIPAA") and regulations promulgated pursuant to HIPAA, as a condition of having access to Personal Information, the parties must first execute a mutually agreeable form of a Business Associate Agreement to protect the privacy of Personal Information constituting "protected health information" within the meaning of HIPAA and HIPAA regulations.

3. Company Compliance with Applicable Laws.

a. Company shall at all times comply its obligations under (i) Privacy Laws that apply to Web.com Personal Information (including without limitation Special Categories of Data), (ii) Privacy Laws to which Company is subject as a service provider Processing Web.com Personal Information or Processor of Web.com Personal Information (including without limitation any Special Categories of Data), or (iii) Privacy Laws that are otherwise applicable to Company's privacy practices in connection with the Services.
b. Company shall not knowingly perform Services or the Agreement in such a way as to cause Web.com to violate any requirement under applicable Privacy Laws.
c. Company shall promptly cooperate with and provide Web.com with the assistance Web.com deems necessary to ensure Web.com Personal Information is Processed as part of Company's Services in compliance with applicable Privacy Laws.
d. To the extent Company creates, receives, maintains, or transmits Personal Data of members of Web.com's workforce as a result of the providing the Services, and Processes that Personal Information as Controller, Company shall at all times comply with its obligations under applicable Privacy Laws as a Controller in relation to such Personal Information.

4. Company Privacy Practices.

a. Company shall develop, implement, maintain, and monitor a comprehensive, written information privacy program to protect the privacy of Personal Information, including Web.com Personal Information. Such program shall include reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of Web.com Personal Information. Such safeguards shall reasonably safeguard Web.com Personal Information from any intentional use or disclosure in violation of this Addendum or applicable Privacy Laws and shall reasonably limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. Company's safeguards shall include any special safeguards needed to protect Special Categories of Data in accordance with applicable Privacy Laws.
b. Company's privacy program shall including implementing one or more privacy policies establishing requirements for providing notification to Data Subjects about the collection, use, sharing, return, deletion or disclosure of Personal Information; providing choices to such Data Subjects about the collection, use, or disclosure of Personal Information; limiting the onward transfer of collected Personal Information; providing Data Subjects access to Personal Information collected about them to afford them the ability to correct, amend, or delete that Personal Information; safeguarding that Personal Information to protect it from loss, misuse, or unauthorized access, disclosure, alteration, or destruction; taking steps to make sure Personal Information continues to be accurate, complete, current, and reliable for its intended use;

establishing mechanisms to investigate privacy complaints or resolve disputes about the handling of Personal Information; and similar Personal Information governance requirements.

c. Company shall train all members of its workforce on its privacy policies and procedures with respect to Web.com Personal Information required by this Addendum, applicable Privacy Laws, and Company's own privacy policies and procedures, as necessary and appropriate for members of Company's workforce to carry out their functions.

d. Upon Web.com's request, Company shall provide the latest version of Company's privacy policies, which Web.com may review and either accept or reject. If Web.com rejects Company's privacy policies, Web.com shall provide a written explanation stating in reasonable detail the respects in which Company's privacy policies are inconsistent with applicable Privacy Laws or otherwise fail to provide adequate protection for the privacy of Web.com Personal Information, and Company shall exercise its best efforts to correct the deficiencies identified by Web.com and resubmit its privacy policies for additional review under this Section. If, within thirty (30) days following Web.com's original written explanation of deficiencies, Company has not corrected or is unable to correct all deficiencies, Web.com shall be entitled, at its sole option, to terminate the Agreement immediately upon notice to Company.

e. Upon Web.com's request, Company shall provide reasonable cooperation and assistance to Web.com in connection with meeting obligations to a Data Subject under applicable Privacy Law to provide such Data Subject a copy of Personal Information relating to the Data Subject, an accounting of disclosures of such Personal Information, or an opportunity to delete, correct, or otherwise amend such Personal Information (or if Web.com or its customer does not agree that it is currently incorrect, to have recorded the fact that the Data Subject considers the data to be incorrect).

f. Company shall, within two (2) business days of receipt, forward to Web.com any request for access, request for an accounting of disclosures, request for an opportunity to amend Personal Information, complaint, notice, or other communication from a Data Subject or a Privacy Authority in connection with Web.com Personal Information (each, a "Communication"). Company shall cooperate with Web.com regarding the Communication and provide reasonable assistance to Web.com in connection with creating a response to the Communication. Company shall not respond to the Communication without Web.com's advance written consent, which shall not be unreasonably withheld. If Web.com is not able to access information requested in the Communication without Company's assistance, Company shall, without charge to Web.com, provide Web.com with any information, in the form in which it is maintained, that is needed to respond to a Communication and is in Company's possession, custody, or control or comply with the rights of Data Subjects under applicable Privacy Laws or mandates from a Privacy Authority.

g. Upon Web.com's request, Company shall provide Web.com with such reasonable information that Web.com, a Web.com customer, or governmental entity may request from time to time to evidence the compliance of Company, a Subcontractor, or other agent of Company with this Addendum or applicable Privacy Law.

h. Company shall ensure that its actual privacy practices conform to the practices described in its privacy policies.

i. Company shall safeguard the privacy and security of the Web.com Personal Information in accordance with Addendum 1 (Security Requirements).

j. Company shall maintain adequate records and logs relating to its Processing and disclosures of Web.com Personal Information and adequate records and logs sufficient to evidence Company's compliance with this Addendum. Upon request, Company shall provide copies of such records and logs to Web.com for the purpose of determining Company's compliance with this Addendum. Web.com shall have the right to conduct such an audit of Company's privacy practices upon thirty (30) days advance written notice not more than twice each year.

5. Right to Access and Correct.

a. Company shall provide Web.com with reasonable access to the Web.com Personal Information in its possession, custody, or control in the format and using the media or transmission mechanism reasonably specified by Web.com. Upon request, Company shall promptly update, correct, or delete Web.com Personal Information in its possession, custody, or control.

b. Upon request of a Data Subject whose Web.com Personal Information Company is Processing, Company shall update or correct Web.com Personal Information relating to such Data Subject, unless Company reasonably believes the Web.com Personal Information is already accurate and complete.

6. Retention and Destruction of Web.com Personal Information. Following the termination of the Services or the Agreement or upon Web.com's request, Company shall promptly comply with Web.com's instructions to return, delete, or destroy all Web.com Personal Information in its possession, custody, or control in accordance with any and all Confidentiality Section(s) of the Agreement. Company shall retain Web.com Personal Information following the termination of the Services only for so long as necessary to comply with such instructions. Following such return, deletion, or destruction, Company shall retain no copies of any Web.com Personal Information, subject to any obligation under applicable evidence preservation law to preserve evidence of a dispute which shall be discharged, if at all, exclusively by Company's counsel and subject to the protections set forth in this Addendum. The foregoing right shall expire when such preservation obligation ends.

7. Exports of Web.com Personal Information.

   a. Company shall inform Web.com of the details concerning each country to which Company proposes to export Web.com Personal Information, including without limitation to a Subcontractor. Company must have Web.com's advance written approvals of transfers to any such countries, which approvals shall not be unreasonably withheld.
   b. Company shall not export Web.com Personal Information constituting EEA Personal Information to a country outside the EEA that does not have an Adequate Level of Protection unless Company enters into and implements an agreement with the Data Importer that incorporates the EU Standard Contractual Clauses by reference.
   c. To the extent Web.com is a Data Exporter and Company is a Data Importer and Web.com Personal Information is exported from the EEA to Company's location in a country without an Adequate Level of Protection, the EU Standard Contractual Clauses are incorporated by reference herein, shall apply to such Web.com Personal Information. To the extent applicable, Company will notify Web.com of any transfer of data outside of the EU. The Parties will agree on the permitted transfer mechanism (i.e. privacy shield certification, Company shall ensure that its workforce and Subcontractors comply with the obligations imposed on the Data Importer in the EU Standard Contractual Clauses in connection with its role as a Processor or sub-Processor of Web.com Personal Information. To the extent there is any conflict between the terms of this Addendum and the EU Standard Contractual Clauses, the terms of the EU Standard Contractual Clauses shall prevail.
   d. Company acknowledges that Web.com may act as (i) a Controller or as a Processor for members of Web.com or (ii) as a Processor for its customers in relation to Web.com Personal Information it receives, that the EU Standard Contractual Clauses apply to the transfer and Processing of such Web.com Personal Information by Company as a Data Importer in its capacity as a Processor or sub-Processor of Web.com or a member of the Web.com Group.
   e. Company shall execute an agreement directly with Web.com incorporating by reference the EU Standard Contractual Clauses in order to comply with EU Standard Contractual Clauses entered into with Web.com Group customers or applicable Privacy Laws.

8. Regulatory Notifications and Approvals.

   a. Company acknowledges that Web.com may need to provide Privacy Authorities with notifications or seek approvals from them in connection with its compliance with the EU Standard Contractual Clauses or applicable Privacy Laws. To the extent necessary in connection with such notifications or approvals, Company hereby authorizes Web.com or any member of the Web.com Group to disclose privacy and security provisions of the Agreement to such Privacy Authorities.

b. Company shall provide Web.com with all reasonable assistance needed in connection with providing notifications to or seeking approvals from Privacy Authorities under subsection (a).