Data Processing and Security Terms

0 Introduction

These Data Processing and Security Terms (these “Terms”) constitute an integral part of the Software-as-a-Service Agreement (the "Software-as-a-Service Agreement") between the Customer and one of the following Web Manuals entities (as applicable “Web Manuals”): (a) Web Manuals Sweden AB, a company incorporated under the laws of Sweden with offices at Nordenskiöldsgatan 6, 211 19 Malmö, Sweden ("WMSAB"); or (b) if the Customer is headquartered in the United States or another country in North or South America, Web Manuals Inc., a company incorporated under the laws of the State of Delaware, USA, with offices at 3300 Admiral Boland Way, San Diego, CA 92101, USA ("WMInc.").

These Terms reflect the parties’ agreement with respect to the processing of Customer Data under the Software-as-a-Service Agreement, including with respect to Customer Personal Data in accordance with the Directive and any applicable national data protection legislation.

These Terms describe the contracting parties’ data protection obligations, information security measures and the minimum data protection standards that Web Manuals shall meet and maintain in order to protect the Customer Data and Customer Personal Data from unauthorized use, access, disclosure, theft, manipulation, reproduction, security breach or otherwise during the term of the Software-as-a-Service Agreement. These Terms apply to all activities, which are related to the Software-as-a-Service Agreement and during which Web Manuals or a Third Party has possession or access to Customer Data and/or Customer Personal Data.

Web Manuals shall use best reasonable effort to ensure that all persons, whom it engages to work on or perform the services under the Software-as-a-Service Agreement or to whom it subcontracts the performance of any of its obligations under the Software-as-a-Service Agreement, comply with the statutory provisions on data protection and keep the Customer Data and Customer Personal Data confidential and secret and not disclose to any third party the Customer Data and/or Customer Personal Data or any part thereof.

1 Definitions

Capitalized terms used but not defined in these Terms will have the meaning set out in the Software-as-a-Service Agreement or its associated Terms and Conditions.

"*Controller*" shall mean 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 Customer Data and/or Customer Personal Data. For the purpose of these Terms, the Customer shall be the Controller.

"*Directive*" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"*Instruction*" is the Customer's written order that addresses how Web Manuals should handle and treat the Customer Data and/or Customer Personal Data in a manner that protects the data (including, but not limited to, creation, updating, de-personalization, blocking, deletion, and return of said data). These Terms constitute the principal Instruction and may be thereafter modified, supplemented or replaced by the Customer through a separate Instruction (Single Instruction). The Customer's Instructions shall be made by an Administrator or other duly authorized person in writing or by e-mail to the Web Manuals Service Desk.

"*Personal Data*" shall mean any information relating to an identified or identifiable natural person ("Data Subject") which is provided to Web Manuals directly or indirectly by the Customer or to which Web Manuals have or gain access from or on behalf of the Customer in connection with the provision of its services for the Customer; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"*Processing*" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"*Processor*" shall mean a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Customer. For the purpose of these Terms, Web Manuals shall be the Processor.

"*Subprocessors*" means the Web Manuals and Third Party Suppliers that process Customer Data and/or Customer Personal Data on behalf of the Customer.

"*Term*" shall mean the full duration of the Software-as-a-Service Agreement during which these Terms are applicable.

"*Third Party*" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the Customer, Web Manuals and the persons who, under the direct authority of the Customer or Web Manuals, are authorized to process the Customer Data and/or Customer Personal Data.

"*Third Party Request*" means a request from a Third Party for records relating to a User's use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the User permitting the disclosure.

"*Third Party Suppliers*" means the third-party suppliers engaged by Web Manuals for the purposes of processing Customer Data in the context of the provision of the Services.

2 Scope

Web Manuals is authorized to perform the subject matter of the Agreement in compliance with these Terms for carrying out all necessary processing steps and uses of the Customer Data and/or Customer Personal Data on Customer's behalf for the following purposes: (i) to comply with Instructions, (ii) to provide the Services (including, but not limited to, publication of files in multiple formats within the context of the Services, duplication of files for protecting against loss, creation of log files, creation of aggregated indexation files, and provision of text search functionality) to the Customer and its Users, and (iii) to otherwise exercise Web Manuals' rights and fulfil its obligations under the Software-as-a-Service Agreement. Any action resulting in the modification of Customer Data and/or Customer Personal Data shall only be performed in accordance with a written Instruction provided by the Customer.

The following categories of data fall within Customer Personal Data: personal data transmitted or displayed by the Customer or its Users via the Services, including user ID numbers or ID codes, contact information, profile images, and any other electronic data uploaded to or created by the Services that can be used to identify a natural person.

The categories of data subjects to which that data may relate include Users of the Services, employees, contractors and the personnel of the Customer and its customers, suppliers and subcontractors. Data subjects may also include individuals whose data the Customer or Users upload to or process via the Services.

Web Manuals shall collect, process, or use the Customer Data and/or Customer Personal Data solely on behalf of the Customer and in accordance with these Terms and with the special Single Instructions issued by the Customer. The processing or use of the Customer Data and/or Customer Personal Data for purposes other than those set forth in these Terms is prohibited.

Web Manuals shall immediately inform the Customer if a Single Instruction given by the Customer does not comply with these Terms. Web Manuals is entitled to suspend the performance of the affected services until the Customer decides on how to continue the Processing of the Customer Data and/or Customer Personal Data.

Web Manuals will confirm Customer's ownership of the stored items to any Third Party in writing if so reasonably demanded by Customer.

3.1 Rights of the data subject

The Data Subjects may enforce their rights against the Customer. The Customer is responsible for safeguarding such rights and is specifically responsible for notifying the Data Subject, providing information to the Data Subject and correcting, deleting and blocking data. The Customer shall promptly notify Web Manuals upon correction, deletion or blocking of data at the request of a Data Subject.

3.2 Third Party Requests

The Customer is primarily responsible for responding to Third Party Requests. Web Manuals will, at the Customer's reasonable expense, and only to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify the Customer of its receipt of a Third Party Request; (b) comply with the Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) if the information is solely held by Web Manuals and reasonably accessible by Web Manuals, provide the Customer with the information or tools required for the Customer to respond to the Third Party Request in a manner consistent with the functionality of the Services. Notwithstanding the foregoing, subsections (a), (b) and (c) above will not apply if Web Manuals determines that complying with those subsections could: (i) result in a violation of Legal Process that Web Manuals or the Customer is a party of; and/or (ii) obstruct a governmental investigation. The Customer will first seek to obtain the information required to respond to Third Party Requests on its own, and will contact Web Manuals only if it cannot reasonably obtain such information.

3.3 Threats to Customer Data and/or Customer Personal Data

If the Customer's data held with Web Manuals is threatened because of possible seizure or confiscation, insolvency or composition proceeding, or other events or transactions of Third Parties, then Web Manuals shall immediately inform the Customer thereof.

Web Manuals shall comply with the ISO 27001 *Information Security Management* standard and applicable laws of data processing and monitor compliance with those principles.

4.1 Security measures

Web Manuals will implement suitable technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss, alteration, or unauthorized disclosure, use or access (the "Security Measures"). Web Manuals may update or modify such Security Measures from time to time provided that (a) such updates and modifications do not result in the material degradation of the security of the Services, and (b) Web Manuals continues to adhere to such Security Measures then in effect. More specific details to the technical and organizational measures taken by Web Manuals are described in Appendix A of these Terms.

All Customer Data and/or Customer Personal Data, including any copies or reproductions made thereof, will be, and shall remain the property of the Customer. Web Manuals shall store such information and materials in accordance with its policies and procedures for maintaining confidential information.

4.2 Training of staff

Web Manuals will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, by means of training as well as maintenance, communication and control of policies and procedures. Furthermore, Web Manuals undertakes to impose confidentiality agreements with any and all personnel employed or contracted for working with Customer Data and/or Customer Personal Data and to instruct such personnel in its data protection and information security policies.

4.3 Compliance audits and security incidents

Web Manuals shall immediately inform the Customer in writing or by e-mail of (i) any compliance audit concerning the Customer Data and/or Customer Personal Data which is to be conducted by data protection authorities, (ii) any material security incident and (iii) any breach or possible breach of data protection in reasonable detail, including, without limitation, the nature of the data compromised, threatened, or potentially compromised.

If and to the extent a compliance audit and/or incident relates to or affects the Customer Data and/or Customer Personal Data or the processing of the Customer Data and/or Customer Personal Data hereunder, Web Manuals will provide the Customer with the final audit and/or incident report when available.

In the event the audit or incident report shows any deficiencies, Web Manuals shall remediate such deficiencies in a timely manner.

4.4 Security Certification

Web Manuals commits to maintain its ISO 9001 and ISO 27001 certifications or comparable certifications for its Services.

5 Customer obligations

The Customer is the owner of the Customer Data and Customer Personal Data and therefore solely responsible for compliance with the statutory provisions of the data protection laws, specifically with respect to the legality of the data disclosure to Web Manuals and the legality of the data processing.

The Customer shall immediately inform Web Manuals in full detail if it discovers errors or irregularities relating the usage or processing of the Customer Data and/or Customer Personal Data.

The Customer shall inform Web Manuals in writing or via e-mail of any change of person or persons, whom it has authorized to issue directives, receive the Customer Data and/or Customer Personal Data and carry out the monitoring.

6 Data Protection Officer

Web Manuals shall, upon request, provide the Customer with the contact data of its company Data Protection Officer who will respond to questions and provide information relating to protection of Customer Data and Customer Personal Data and related issues.

Web Manuals' Data Protection Officer shall use reasonable endeavors to secure compliance with applicable laws and regulations concerning data protection. If the Data Protection Officer identifies irregularities in the processing of the Customer Data and/or Customer Personal Data hereunder, then clause *4.3 Compliance audits and security incidents* of these Terms will apply.

Upon request, Web Manuals will provide the Customer with a summary of all information and findings contained in latest audit report and other documents prepared by Web Manuals' Data Protection Officer which relate to the processing of the Customer Data and Customer Personal Data hereunder.

7 Customer's monitoring rights

The Customer's company Data Protection Officer and/or persons named by the Customer perform and audit Web Manuals' place of business in accordance with the *Web Manuals Terms and Conditions for Software-as-a-Service* clause *4.6 Auditing of supplier* and check on the reasonableness of the measures taken to comply with the technical and organizational requirements of the data protection laws applicable to processing of the Personal Data.

8 Subcontractors

Web Manuals has the right to use Third Party Suppliers for the fulfillment of the duties stipulated in these Terms in accordance with the *Web Manuals Terms and Conditions for Software-as-a-Service* clause *3.5 Subcontractors*. The Customer consents to Web Manuals subcontracting the processing of Customer Data and Customer Personal Data to Subprocessors. Web Manuals' liability for any and all actions of Subcontractors it elects to hire or use for the fulfillment of this Agreement as Subprocessors is defined in *Web Manuals Terms and Conditions for Software-as-a-Service* clause *10.3 Limitation of Liability*.

At the written request of the Customer, Web Manuals will provide additional information regarding Third Party Suppliers and their locations. The Customer may send such requests to Web Manuals' Data Protection Officer.

9 Deletion of Customer Data

Upon termination or expiration of these Terms or upon written request by Customer, Processor shall immediately cease processing the Customer Data and Customer Personal Data. Furthermore, Customer Data and Customer Personal Data shall be deleted in accordance with the *Web Manuals Terms and Conditions for Software-as-a-Service* clause *9.5 Responsibility for Content at termination*.

The aforementioned does not apply to any written correspondence or to other documents and written materials which by law must be retained or to written materials which have been designated for retention with Web Manuals. In the event and to the extent that the applicable mandatory law imposes stricter obligations regarding the deletion of the Customer Data and/or Customer Personal Data than under these Terms, the applicable law shall prevail.

A Appendix A: Security Measures

As of the Effective Date, Web Manuals complies with the Security Measures set out in this Appendix.

These specifically include the following measures:

- to prevent unauthorized persons from gaining physical access to data processing facilities where Customer Data and/or Customer Personal Data are processed and used (physical access monitoring);
- to prevent unauthorized persons from being able to use the data processing systems (systems access monitoring);
- to ensure that the persons authorized to use a data processing system have access only to the data which they have the authority to access and that the Customer Data and Customer Personal Data cannot be read, copied, altered or removed without authorization during the processing, use or following the storage thereof (data access monitoring);
- to ensure that the Customer Data and Customer Personal Data are not read, copied, altered or removed without authorization during the electronic transmission or transport or data carrier backup thereof and that it will be possible to review and determine which bodies have been envisaged as the recipient of Customer Data and/or Customer Personal Data transfer by way of data transmission facilities (disclosure monitoring);
- to ensure that it will be possible to review and determine after the fact whether and by whom Customer Data and/or Customer Personal Data was entered into, modified in or removed from data processing systems (input monitoring);
- to ensure that Customer Data and/or Customer Personal Data can be processed only in accordance with the Customer's Instructions (job monitoring);
- to ensure that the Customer Data and Customer Personal Data are protected against accidental destruction and loss (availability monitoring);
- to ensure that data collected for different purposes can be processed separately (separation monitoring).

A1.1 Data Centers

A1.1.1 Infrastructure

Web Manuals employs geographically distributed data centers ("Data Centers") owned and managed by a contracted supplier. Web Manuals stores all production data in physically secure Data Centers. If the Customer has entered into agreement with WMSAB, the Customer's data will be stored within the EU.

A1.1.2 Redundancy

The Data Centers are equipped with an infrastructure that has been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Web Manuals to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the Data Centers' equipment is scheduled through a standard change process according to documented procedures.

A1.1.3 Power

The Data Center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. A primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the Data Center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the Data Center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the Data Center at full capacity typically for a period of days.

A1.1.4 Server Operating Systems

Web Manuals servers use a Linux-based implementation customized for the application environment. The servers are maintained on a regular basis to ensure that security and stability patches are implemented in a timely manner.

A1.1.5 Businesses Continuity

Web Manuals creates backups of data over multiple locations to help to protect against accidental destruction or loss. Web Manuals has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

A1.2 Networks and Transmission

A1.2.1 Data Transmission

Data Centers are connected to the Internet via high-speed IP networks to provide secure and fast data transfer. The Web Manuals application transfers data via secure standard Internet protocols.

A1.2.2 External Attack Surface

Web Manuals employs multiple layers of network devices and intrusion detection to protect its external attack surface. Web Manuals considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

A1.2.3 Intrusion Detection

Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Web Manuals intrusion detection involves:

1. tightly controlling the size and make-up of Web Manuals' attack surface through preventative measures;
2. employing automated detection controls at data entry points; and
3. employing technologies that automatically remedy certain dangerous situations.

A1.2.4 Incident Response

Web Manuals operates a number of methods for availability monitoring and qualified technical personnel available 24 hours a day, 7 days a week, will react promptly to incidents affecting availability.

A1.2.5 Encryption Technologies

Web Manuals employs HTTPS encryption (also referred to as SSL or TLS) to all web-based Services.

A2.1 Site Controls

A2.1.1 Data Center Security Operation

The Data Centers maintain a security operation responsible for all physical Data Center security functions 24 hours a day, 7 days a week. The security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems.

A2.1.2 Data Center Access Procedures

The Data Centers maintains formal access procedures for allowing physical access to the Data Centers. The Data Centers are housed in facilities that require electronic card key access, with alarms that are linked to the security operation. All entrants to the Data Center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the Data Centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data Center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the Data Center director. All other entrants requiring temporary Data Center access must: (i) obtain approval in advance from the Data Center managers for the specific Data Center and internal areas they wish to visit; (ii) sign a Non-Disclosure Agreement, and (iii) reference an approved Data Center access record identifying the individual as approved.

A2.1.3 On-site Data Center Security Devices

The Data Centers employ an electronic access control system that is linked to a system alarm. The access control system monitors and records each individual's access key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and Data Centers is restricted based on zones and the individual's job responsibilities. The fire doors at the Data Centers are alarmed. CCTV cameras are in operation at the Data Centers. The positioning of the cameras has been designed to cover strategic areas. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week.

A2.2 Access Control

A2.2.1 Infrastructure Security Personnel

Web Manuals has, and maintains, an information security policy for its personnel, and requires security training as part of the training package for its personnel.

A2.2.2 Access Control and Privilege Management

Customer's administrators must authenticate themselves via an authentication system in order to administer the Services.

A2.2.3 Internal Data Access Processes and Policies – Access Policy

Web Manuals' internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data and Customer Personal Data. Web Manuals aims to design its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data and/or Customer Personal Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.

Web Manuals requires the use of unique user IDs, strong passwords, two-factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need-to-know-basis; and must be in accordance with Web Manuals' internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

To ensure the security of Customer data on employee computers, Web Manuals encrypts on-board storage devices that require hardware tokens to access data.

A3.1 Data Storage, Isolation and Logging

Web Manuals stores the Customer's data in a multi-tenant environment on virtual servers. The Web Manuals Services logically isolate the Customer's data. The Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable the Customer to determine the data sharing settings applicable to Users for specific purposes. Customer has access to logging capabilities that Web Manuals makes available via the Services.

A3.2 Decommissioned Disks and Disk Erase Policy.

Certain disks containing data may experience performance issues, errors or hardware failures that lead them to be decommissioned. Every Decommissioned Disk is subject to a data destruction process before leaving the Data Center's premises either for reuse or destruction.

A4 Personnel Security

Web Manuals personnel are required to conduct themselves in a manner consistent with the company's policies regarding confidentiality and information security, business ethics, appropriate usage, and professional standards. Web Manuals conducts reasonably appropriate background checks as a part of the company's recruitment process, to the extent legally permissible and in accordance with applicable local labor law.

Personnel are required to sign a confidentiality agreement and must acknowledge receipt of, and compliance with, Web Manuals' confidentiality and privacy policies. All personnel participate in information security training. Personnel handling customer data are required to complete additional Service Desk and/or Service Development training appropriate to their role and prove their proficiency according to company standards. Web Manuals' personnel will not process Customer Data without authorization.

A5 Subprocessor Security

Prior to contracting new Subprocessors, Web Manuals conducts an audit of the security and privacy practices of the Subprocessors to ensure that the Subprocessors provide a level of security and privacy appropriate to their access to Customer Data and the scope of the services they are engaged to provide. Once Web Manuals has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy agreements.