Date of last update: 17 January 2022

Part 1
Data Security

Except as expressly provided, words and expressions in this document shall have the same meaning assigned to them in the relevant end-user licence agreement between Avvoka Limited and the customer entered into from time to time.

1 Introduction

1.1 This document sets out the minimum security requirements that the Provider and its Approved Sub-Processors must adhere to in relation to the processing of Customer Personal Data.

2 Minimum Security Requirements

The Provider shall, by itself, and shall ensure that all of its Approved Sub-Processors, at all times comply with the following minimum security requirements:

3 Availability

3.1 The Provider’s Software is hosted on servers operated by OVH.com or aws.com (as elected by the Customer in writing prior to the Effective Date). Access to each data centre is strictly controlled and monitored using a variety of physical controls, intrusion detection systems, environmental security measures, 24 x 7 on-site security staff, biometric scanning, multi-factor authentications, video surveillance and other electronic means.

3.2 All physical and electronic access to each data centre by its employees is authorised strictly on a least privileged basis and is logged and audited routinely.

3.3 The Provider’s employees do not have physical access to the servers. Electronic access to the servers and services is restricted to a core set of approved OVH.com or aws.com staff only.

3.4 By default, the Provider’s servers are equipped with automatic DDoS attack mitigation in the event of an attack (reactive mitigation). The Provider’s servers use Cisco antivirus software that is built for Linux OS and covers the detection and quarantine of malware, viruses and trojans. All the Provider’s employees have Provider-controlled anti-virus installed on their machines in accordance with the Provider’s information security policy.

4 Integrity and Confidentiality

4.1 Access to the Software is restricted to authorised users that have registered with an email address and password. Two-phase authentication is available, as is single-sign-on, upon Customer request and settlement of payment.

4.2 The connection to the Software (including API access) is secure and encrypted using HTTPS. Documents on the Software are also stored and encrypted at rest using AES – 256 bit encryption.

4.3 Each database value is encrypted with a unique initialisation vector. As an additional safeguard, each key is encrypted with a regularly rotated master key.

4.4 All document data is replicated and regularly backed up. All backups are encrypted using AES-256 with random daily encryption keys.

5 Transparency

The Customer is able to nominate individuals to access the Software as “organisational” administrators, enabling such individuals to view all of the data relating to its user’s activity on the Software. The Provider also provides its policies around handling of Personal Data which are compliant with ISO 27001 standards.

6 Isolation

6.1 The Provider employs strict controls around the Software to ensure that only individuals with the appropriate legitimate interest are able to access Personal Data. There is a hierarchy of support roles around user administration ensuring that “administrators” with pre-agreed clearance are able to manage Customer Data. The following hierarchy applies:

(A) System administrators - Provider’s nominated support employees that are able to manage information relating to all user accounts (e.g. management of usernames, e-mail addresses and high-level details of documents created by users of the Software)

(B) Organisational administrators - Customer’s nominated support employees that are able to manage information relating to their own user accounts only (e.g. management of usernames, e-mail addresses and high-level details of documents created by users of the Software)

(C) Profile administrators - Customer’s nominated support employees at a local (e.g. team-level) that are able to manage information relating to their own team’s user accounts only (e.g. management of usernames, e-mail addresses and high-level details of documents created by users of the Software)

Non-administrator users of the Software have no access to any other user data but their own.

7 Intervenability

The Customer is able to nominate individuals to access the Software as “organisational” administrators, enabling such individuals to manage the processing of Customer Data, including Personal Data relating to Data Subjects.

Part 2
Data processing, purpose and subjects

1 The Provider will be processing the Customer Personal data on behalf of the Customer for the purpose of providing the Services under the relevant end-user licence agreement.

2 The Provider will be processing the Customer Personal Data on behalf of the Customer for the duration of the Term and:

(A) documents generated by or on behalf of the Customer on the Software that are not electronically signed using the Software shall not be erased automatically, unless otherwise agreed by the Parties;

(B) documents generated by or on behalf of the Customer on the Software that have been electronically signed using the Software shall be retained indefinitely unless the Customer and the relevant counterparties to the document notify the Provider in writing to erase such document (together with all associated user Personal Data relating thereto); and

(C) subject to paragraph 2(A) above, files uploaded to the Software by or on behalf of the Customer or its clients shall remain the sole responsibility of the Customer and shall remain on the Software until they are erased by the Customer in accordance with the Customer's own data protection policies.

3 The Provider will be processing the following types of Personal Data: names of individuals; trading / business names; salutations; postal and email addresses; telephone (including mobile telephone) numbers and any other Personal Data provided to the Provider by the Authorised Users in connection with the Services.

4 The Provider will be processing Personal Data of the following categories of Data Subjects: (i) employees, agents and representatives of the Customer; and (ii) actual and potential customers and clients of the Customer.