TECHNICAL AND ORGANIZATIONAL SECURITY – SCHEDULE 5

1. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Schedule 5 describes certain technical and organizational security measures that we have implemented in accordance with applicable laws, rules, treaties, and governmental regulations, including without limitation applicable Data Protection Laws as they apply to the provision of the Services and as directed by Customer. All terms, capitalized or otherwise, that are used in this Schedule 5 that are defined in Schedule 4, shall have the meanings ascribed to such terms in Schedule 4. Taking into account the state of the art, the costs of implementation, and the nature, scope, content, and purpose of the processing, we represent and warrant that we have implemented the data security measures described below. Our information security management system is certified for compliance with the ISO/IEC 27001 standard.

1.1. Physical Access

All databases, application servers, and related hardware used to power our systems are hosted in a secure AWS cloud. Physical access to those devices is controlled by Amazon according to industry best practices and standards.

1.2. Virtual Access

Access to infrastructure and processing resources are secured by Virtual Private Networks (VPNs). Access to our VPNs is limited to our personnel who require access to perform their job functions.

Technical and organizational measures are in place to prevent unauthorized persons from virtually accessing our systems, including:

- Establishing user identification and authentication procedures;
- Establishing ID/password security procedures (special characters, minimum length, change requirements);
- Ensuring that admission to data processing systems is only possible after identification and authentication using the correct ID and password for the particular system;
- Using automatic blocking by timeout;
- Monitoring intrusion attempts and automatically blocking user upon several erroneous password attempts;
- Creating one master record per user;
- Using firewalls; and
- Implementing encryption for data at rest and in transit where needed.

1. DATA ACCESS

Technical and organizational measures are in place to ensure that persons entitled to use a data processing system gain access only in accordance with their access rights and that personal data cannot be read, copied, modified, or deleted without authorization, including:

- Establishing written internal policies and procedures;
- Ensuring that personal data necessary for the performance of the particular task is limited within the systems and applications by a corresponding role and authorization framework,

which allows access to employees on a "need to know" basis, ensuring that each role has only such access rights as are necessary to fulfill the task to be performed by that specific person;

- Establishing control authorization schemes;
- Establishing differentiated access rights (Role Based Access Control);
- Monitoring and logging of access;
- Encryption, the suitability of an encryption technology is evaluated by reference to its protective purpose.

2. DISCLOSURE AND TRANSMISSION

The measures necessary to ensure the security of personal data during processing and transmission are described in our information security policies and are implemented in accordance with a risk-based security classification system. We transfer Customer Personal Data to third parties in accordance with the Customer's instructions and this Agreement and enter into a written agreement with such third parties in accordance with applicable Data Protection Laws. Customer Personal Data will not be stored or processed using non-secure or non-professional systems (e.g., public cloud systems).

3. OTHER CONTROLS

Technical and organizational measures are in place:

- to monitor whether personal data may have been entered, changed, or removed (deleted), and by whom, from data processing systems, including logging and reporting systems and audit trails and documentation,

- to ensure that personal data are processed solely in accordance with the instructions of Customer, including the Agreement, and this Schedule, and

- to ensure that personal data are protected against accidental destruction or loss (physical/logical), including:

    - Establishing backup procedures;
    - Establishing a Disaster Recovery Plan;
    - Establishing a Business Continuity Plan.

- to ensure that personal data collected for different purposes can be processed separately, including:

    - Logical separation;
    - Establishing parameters for limitation of use;
    - Segregating functions (production/testing/development); and
    - Establishing procedures for separate storage, amendment, deletion; transmission of data for different purposes.

4. INFORMATION CLASSIFICATION

4.1. **Owners and Production Information** - All electronic information that we manage and process has a designated Owner. Production information is information routinely used to accomplish business objectives. Owners are at the Director level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Senior or Executive Management team who act as stewards, and who supervise the ways in which each type of information is used and protected.

4.2. **Public** - Information Assets are classified as “Public” if we make the explicit decision to share them with the public. This classification may only be applied by business units that are authorized to do so.

4.3. **Internal Use** - This category applies to most of the information that we manage; this is information required and created as part of our day-to-day activities. Internal Use information may be shared with our employees and contractors, and with third parties. However, when we share information or communicate with third parties, we take precautions to ensure protection of the confidentiality of the information where applicable.

4.4. **Confidential** - This category applies to sensitive information that could cause damage if shared with unauthorized parties. Information Assets that contain Personal Data (including name, phone number, physical address, email address, and any other data relating to an identifiable individual) must be classified as Confidential – Personal Data. Confidential Information may be shared with our employees and contractors; and third parties that have signed a nondisclosure agreement (NDA). The owner and the recipients of Confidential Information assets distributed in any form (paper, electronic, verbal) assume responsibility for limiting the distribution. In electronic form, Confidential Information must be subject to technical controls, when available, ensuring that the owner controls who has access to the information.

4.5. **Highly Confidential** - This applies to very sensitive information that would cause serious damage if shared with unauthorized parties. Information Assets that contain Sensitive Personal Data should be classified as Highly Confidential – Sensitive Personal Data. Highly Confidential Information Assets may be shared with our employees and contractors; and third parties that have signed a non-disclosure agreement. Highly Confidential Information Assets in electronic form are subject to additional technical controls, when available, ensuring that only predefined individuals can access the information. Highly Confidential Information Assets in paper form may be shared only with a pre-defined group of individuals.