TECHNICAL AND ORGANIZATIONAL SECURITY
SCHEDULE 5

1. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES.

This Schedule 5 describes certain technical and organizational security measures that SocialEdge has 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, SocialEdge represents and warrants that it has implemented the data security measures described below.

1.1. Physical Access

All databases, application servers and related hardware used to power SocialEdge systems are hosted in secure AWS and Azure clouds. Physical access to those devices is controlled by Amazon and Microsoft respectively and conforms with state-of-the-art best practices.

All SocialEdge data and processing resources are secured by Virtual Private Networks (VPNs). Access to SocialEdge VPNs is limited to SocialEdge personnel that requires this access to perform their job functions.

1.2. Virtual Access

Technical and organizational measures to prevent unauthorized persons from virtually accessing SocialEdge's systems, including:

1.1.1. Establishing user identification and authentication procedures;
1.1.2. Establishing ID/password security procedures (special characters, minimum length, change requirements);
1.1.3. Ensuring that admission to the data processing systems is only possible after identification and authentication using the correct identification code and password for the particular system;
1.1.4. Using automatic blocking (e.g., password or timeout);
1.1.5. Monitoring intrusion attempts and automatically turning off user ID upon several erroneous passwords attempts;
1.1.6. Creating one master record per user, user master data procedures, per data processing environment;
1.1.7. Using firewalls and proxy servers; and
1.1.8. Implementing encryption and pseudonymization as appropriate. Suitability of an encryption technology is evaluated by reference to its protective purpose.

2. DATA ACCESS.

Technical and organizational measures 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;

2.1. 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 fulfil the task to be performed by that specific person;

2.2. Establishing control authorization schemes;

2.3. Establishing differentiated access rights (profiles, roles, transactions and objects);

2.4. Monitoring and logging of access;

2.5. Encryption and pseudonymization, as appropriate. Suitability of an encryption technology is evaluated by reference to its protective purpose.

3. DISCLOSURE AND TRANSMISSION.

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

4. OTHER CONTROLS.

Technical and organizational measures 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.

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

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

4.1. Establishing backup procedures;

4.2. Mirroring hard disks;

4.3. Ensuring uninterruptible power supply;

4.4. Using remote storage;

4.5. Using anti-virus/firewall systems; and

4.6. Establishing a disaster recovery plan.

SocialEdge ensures the availability of its data processing systems themselves in accordance with the necessary security level by corresponding security measures.

Technical and organizational measures to ensure that personal data collected for different purposes can be processed separately, including:

4.7. Separating databases;

4.8. Establishing parameters for limitation of use;

4.9. Segregating functions (production/testing); and

4.10. Establishing procedures for separate storage, amendment, deletion; transmission of data for different purposes.

5. Data Classification

5.1. **Owners and Production Information**—All electronic information managed and processed by SocialEdge must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be 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.

5.2. **RESTRICTED**—This classification applies to SocialEdge's most sensitive business information. Its unauthorized disclosure could seriously and adversely impact SocialEdge, its investors, its customers, its business partners, and/or its suppliers. Restricted information includes any data that is deemed personally identifiable or PII information under applicable laws, including name, phone number, physical address, email address, and any other data relating to an identifiable individual, as well as any other information provided to SocialEdge by customers (subject to any applicable non-disclosure provisions). Personal data for which another party is data controller may be shared only with that party or as agreed with that party.

5.3. **CONFIDENTIAL**—This classification applies to less-sensitive business information that is intended for use within SocialEdge, but which may, with permission and/or authorization from Data Owners, be shared externally, subject to defined restrictions on recipients and/or purposes. Its unauthorized disclosure could adversely impact SocialEdge or its investors, customers, suppliers, business partners, or employees. Information that is generated by or prepared for customers including within the specific customer instance within the SocialEdge platform, is deemed as "Confidential" as it is intended for sharing with that customer. Personally identifiable information or personal data is always deemed as "Restricted".

5.4. **PUBLIC**—This classification applies to information that has been approved by SocialEdge management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

5.5. **Owners and Access Decisions**—Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information, and that these controls are monitored and kept up to date.