INFORMATION SECURITY POLICY

[Last updated: September 17, 2020]

The International Renewals Group ("**Company**", "**we**" or "**us**") is committed to provide transparency regarding its security measures and policies which it has implemented in order to secure and protect the personal data and personal information (as such terms are defined under applicable data protection law including without limitations, the EU General Data Protection Regulation ("**GDPR**") and the California Consumer Privacy Act ("**CCPA**") (collectively, the "**Data Protection Regulations**")) (collectively. "**Personal Data**") of those individuals whose Personal Data the Company processes. As such, the Company created this information security policy ("**Security Policy**") to disclose the ways that it safeguards Personal Data processed through its services ("**Service(s)**"). We have implemented the below technical and organizational measures to protect the Personal Data, processed by us, against loss, unlawful acts and destruction, alteration, unauthorized disclosure or access, etc.

As part of the Company's data protection compliance process the Company has implemented technical, physical and administrative security measures to protect the Personal Data and has prepared this Security Policy to provide you with a summary of the security measures and policies it upholds. The Company also requires its partners and employees to comply with these standards and implement the same security measures when working with it.

THIS SECURITY POLICY OUTLINES THE COMPANY'S CURRENT SECURITY, TECHNICAL AND ORGANIZATIONAL PRACTICES AS OF THE "LAST UPDATED" DATE INDICATED ABOVE. WE WILL CONTINUE TO UPDATE THIS SECURITY POLICY FROM TIME TO TIME, AS REQUIRED BY APPLICABLE LAWS AND OUR INTERNAL POLICIES.

SYSTEM ACCESS CONTROL

The Company's database can only be accessed by a minimum amount of Company employees and personnel and only from within the Company's office. The Personal Data is provided to employees on a need-to-know basis. The Personal Data is processed and stored by the Company through cloud services and access to such is granted through personal user authentication. Access to systems is restricted and there are procedures in place to ensure that the appropriate approvals are only provided to the extent required (including logins). Each computer has its own applicable login. In addition, remote access and wireless computing capabilities are restricted and require both user and system safeguards. The systems are also protected and only authorized employees may access the systems by using a designated password and user names. All emails have a two-step verification security process.

PHYSICAL ACCESS CONTROL

The Company secures any and all physical access to its offices and ensures that only authorized individuals have access to its offices (for example: its employees). All employees are provided a personal key to be able to enter the Company's offices. All visitors and individuals who are not a part of the Company are escorted by a Company employee during the entire time that they are on the Company's premises. The Company works with Amazon Web Service's datacenter and it is its main storage processor. We therefore advise you to review Amazon's security policy that is available here for more information.

DATA ACCESS CONTROL

All access to any of the Company's databases, systems or storage units may only be done with an authorization hierarchy and password protection. Furthermore, as mentioned above, access to the Personal Data is restricted to those employees with a "need to know" and is protected through passwords and user names. Access to the Personal Data is secured and is strictly managed with access control policies. Only the Company's upper management has access and full control over the data systems. The Company uses high level security measures to ensure that the Personal Data will not be accessed, modified, copied, used, transferred or deleted without specific authorization. The Company audits any and all access to the databases and any authorized access is immediately reported and handled. Each employee is only able to perform tasks and take actions in accordance with his or her authorizations that are determined by the Company. Each time someone accesses a database or system it is logged and monitored, and any unauthorized access is automatically reported. Furthermore, the Company performs an ongoing review of which employees' have authorizations, to assess whether access is still required. The Company revokes an employee's authorizations immediately upon such employee's termination of employment. Authorized individuals can only access Personal Data that is included in their individual profiles.

TRANSFER CONTROL

The purpose of transfer control is to ensure that Personal Data cannot be read, copied, modified or removed by unauthorized parties during the electronic transmission of such Personal Data or during the transport or storage of such Personal Data in the applicable data center. Furthermore, any and all transfers of the Personal Data (either between the servers, from client side to server side and between Company's designated partners) is secured (HTTPS) and encrypted.

DATA RETENTION

Personal Data and raw data are all deleted as soon as possible or as required under applicable law.

ORGANIZATIONAL AND OPERATIONAL SECURITY

The Company educates its employees and service providers, consultants and contractors and raises awareness, risks and conducts assessments with regards to any processing of Personal Data. Internal security testing is done on a regular basis. The Company's IT team ensures security of all hardware and software by installing anti-malware software on computers to protect against malicious use and malicious software as well as virus detection on endpoints, email attachment scanning, system compliance scans, information handling options for the data exporter based on data type, network security, and system and application vulnerability scanning, use secured email transfer, etc. It is the responsibility of the individuals within the Company to comply with these practices and standards.

AVAILABILITY CONTROL

The Company's servers include an automated backup procedure. The Company has a backup policy which includes automated daily backups. The Company conducts periodic checks to determine that the backups have occurred. The Company has ensured that all documents, including without limitations, agreements, privacy policies online terms, etc. are compliant with the applicable Data Protection Regulations. Our legal team has ensured our legal documentation is updated to reflect any changes and to include the mandatory provisions required by the applicable Data Protection Regulations.

JOB CONTROL AND CONTRACTUAL OBLIGATIONS

Employees, customers, vendors and applicable processors are all signed on binding agreements all of which include applicable data protection provisions and data security obligations. As part of the employment process, employees undergo a screening and are provided with access to the database during his or her training to ensure he or she is well educated and responsible to handle the Personal Data. Employees are required to comply with this Security Policy in addition to our internal security policies and procedures and breaking or not complying with such shall result in disciplinary actions. The Company conducts annual compliance training which includes data security education in order to ensure the employees stay educated and up to date with applicable policies and legislation.