



Last Updated on April 10th, 2021

## **Dynamic DMC GDPR Compliant Privacy Policy**

### **1. Data Security**

Dynamic DMC warrants it and its employees, contractors and agents will take all actions necessary to insure confidentiality and will use compliance strategies and security risk control practices with respect to the handling of data collected for the purpose of program operation, including the handling of such data by its employees, agents and network technology. Data (known as “Personal Data”) will be defined as, but is not limited to, social security numbers, passport numbers, debit/credit card information and numbers, driver’s license numbers, financial account information, names and addresses.

GDPR:

Notwithstanding anything to the contrary, with regard to the Client personal data which Dynamic DMC processes in connection with any of its Agreements, as those terms are defined by the General Data Protection Regulation, or “GDPR”, Dynamic DMC covenants that DMC will comply with the requirements of the GDPR, as amended, and Dynamic DMC will not cause the Client to fail to comply with the GDPR in connection with this Agreement. Specifically, but without limitation, the parties agree that the Standard Contractual Clauses adopted by the European Commission for the transfer of personal data from data controllers in the EU to data processors in jurisdictions outside the European Economic Area contained in Decision 2010/87/EU are incorporated by reference as if set forth herein in full. Further, Dynamic DMC agrees to:

- Only act on the written instructions of the Client, and process the Client personal data strictly as necessary to perform the services which are the subject of this Agreement;
- ensure that Dynamic DMC personnel, including but not limited to employees, temporary workers and agency workers, who may process the Client personal data are subject to confidentiality agreements with restrictions at least as protective of the Client as those contained herein;
- to protect the Client personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access and, in particular, where the processing involves the transmission of data over a network, against all other



unlawful forms of processing. Having regard to the state of the art and cost of their implementation, Dynamic DMC further agrees that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the Client personal data to be protected.

- Only engage sub-processors with the prior consent of the Client and under a written contract which includes confidentiality restrictions at least as protective of the Client as those contained herein;
- act in good faith to assist the Client in providing data subject access and allowing data subjects to exercise their rights under the GDPR;
- act in good faith to assist the Client in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the Client as requested at the end of this Agreement; and submit to audits and inspections, provide the Client with whatever information it needs to ensure that each party is meeting their obligations under Article 28 of the GDPR, and notify the Client immediately in writing if Dynamic DMC is asked to do something which may violate the requirements of the GDPR or other data protection law of the EU or a Member State.

DMC further warrants that it will:

- a) Continually monitor and protect all Personal Data and will destroy, in a secure fashion, all Personal Data when no longer needed.
- b) Limit access to Personal Data to only those employees, agents and contractors that have a need to know such information to conduct business pursuant to this Agreement. Comply with industry accepted security and data protection practices, including, but not limited to, ensuring data is protected, systems are backed up, patches are current, virus scanning is up to date and run regularly.
- c) Maintain a log of individuals who have access to Personal Data.
- d) Immediately notify the Client of any security breach or unauthorized access of Personal Data.
- e) Allow the Client the right to monitor security practices and/or conduct an audit of DMC security practices, procedures, controls and logs.
- f) DMC will protect SPI and ensure data is encrypted during transmission and storage.
- g) If Client shares charge card information, DMC will maintain PCI compliance



certification appropriate to its tier of merchant transactions and will provide Client with its Attestation of Compliance upon request. DMC agrees to indemnify and hold harmless Client, individual participants and the Client with regard to any breach of its obligations with regard to Personal Data.

05 Hoja Blanca St, San Antonio Escazú, San José, Costa Rica  
+(506) 2288-4318  
info@dynamicdmc.com  
www.dynamicdmc.com

