FOR OUR EUROPEAN CONTACTS WHO RECEIVE MARKETING COMMUNICATIONS:

GENERAL DATA PROTECTION REGULATION (GDPR) POLICIES AND PROCEDURES

(EFFECTIVE MAY 25, 2018)

TABLE OF CONTENTS

1.0 Definitions

General Data Protection Regulation (GDPR) is a regulation in European Union (EU) law on data protection and privacy for all individual persons within the European Union. GDPR is directly applicable to each Member State. It also addresses the export of personal data outside the EU. The GDPR replaces the 1995 Data Protection Directive.

Data Subject means an identified or identifiable natural person who is physically in the European Union.

Personal Data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Data Protection Authorities (DPA) are appointed by each nation and are responsible for enforcing data protection laws at a national level and providing guidance on the interpretation of those laws.

Data Protection Commissioner (DPC) is the head of each nation's Data Protection Authority who is ultimately responsible for upholding the rights of individuals and enforcing the obligations on controllers as set out in the GDPR.

2.0 Data Protection Officer

A Data Protection Officer (DPO) is to ensure that our organization processes the personal data of its staff, customers, providers, or any other individuals (data subjects) in compliance with the applicable data protection rules. Our DPO is as follows:

Jennifer Guenther, Esq.
General Counsel/Director
650 E. Hospitality Lane, Suite 125
San Bernardino, CA 92408-3508

888.826.5814

DPO@adec-innovations.com

3.0 Data Protection and Privacy Policy

3.1 Who we are

FCS International, Inc. dba ADEC Innovations and dba FirstCarbon Solutions is a corporation registered in California, U.S.A.

Business Entity contact information:

All business entities identified above can be contacted by reaching out to GDPR@adec-innovations.com, or contacting the Data Protection Officer.

FCS International, Inc. advances sustainable practices around the world and helps organizations responsibility grow and operate their business through environmental services and analysis, data management, consulting, software as a service, and related services and support.

3.2 How we comply with GDPR for data subject requests

When we receive requests for assistance from data subjects, we will comply with the requests to the best of our ability, within the appropriate timeframe. If we are unable to comply with a request or if fulfilling the request will take additional time, we will provide notice of the same to the data subject in a timely manner.

3.3 Who can data subjects contact regarding our GDPR compliance?

For convenience, our family of companies has established a single point of contact for any inquiries regarding GDPR.

Our DPO is:

Jennifer Guenther, Esq.
General Counsel/Director
650 E. Hospitality Lane, Suite 125
San Bernardino, CA 92408-3508

888.826.5814

DPO@adec-innovations.com

3.4 Who is collecting data and why?

Our marketing team collects personal data of individual data subjects from public sources, through our software applications, and with the use of marketing software to provide customers and potential customers with content relevant to their industry and business contacts.

We process the marketing data collected to provide context for sending relevant industry, product and company communications. Data storage is discussed further below in this policy.

Once you have opted to receive our communications, our marketing database may include the following information to allow us to contact you to provide relevant, industry specific content:

Company Name – Used to help us address you properly and to help deliver industry specific content.

Individual Name – Used to communicate with you and as a way to find your information in our system.

Salutation – Used to help us address you properly in our communications.

Mailing Address – Used for sending notifications, messages, and content. Also used to deliver geographically relevant content and assign internal team responsibilities.

Email Address – Used for sending notifications, messages, and content.

Job Title – Used to help us address you properly in our communications, to identify your organizational role, and to help deliver specific content.

Industry Focus – Used to help us deliver relevant content to you.

Telephone Number – Used if we need to contact you by phone.

Company Type – Used to help focus the content on your area of interest.

3.5 To whom will the data be disclosed? Any third parties?

When data is entered into our system, the information may be received by one or more of our following teams:

Marketing Team – Located in Irvine, California and Hamburg, New Jersey, U.S.A.

Marketing Support Team – Kingston, Philippines

Marketing Team Director – Weed, California, U.S.A.

Customer Success Team – located in Irvine, California, U.S.A.; Sacramento, California, U.S.A.; Walnut Creek, California, U.S.A.; Gloucestershire, UK

Product Management Team – located in Irvine, California; Pittsburgh, Pennsylvania; and Phoenix, Arizona, U.S.A.

When the information is received by our teams, each does the following with it:

Marketing Team – assigns contacts to appropriate teams and distribution lists, and/or responds to inquiry

Marketing Support Team – assigns contact to appropriate teams and distribution lists

Marketing Team Director – responds to inquiry

Customer Success Team – responds to inquiry

Product Management Team – responds to inquiry

Please note that individual names of our employees are omitted from this policy because while employees and their responsibilities can and do change, the teams responsible and the duties of those teams do not change with the same frequency. This is our way to keep these policies simple and accurate for you.

3.6 Will data leave the European Economic Area?

Yes. Our marketing data is transferred outside the European Economic Area. Marketing data will be processed and stored using HubSpot, Inc., and data will also be collected, processed, and stored using SurveyMonkey.

The HubSpot platform is hosted in the United States and HubSpot uses Amazon Web Services (AWS) in Northern Virginia, U.S.A. (US-East 1 region) to store its data. Both HubSpot, Inc., and AWS represent they maintain an audited security program including SOC 2 and ISO 27001 compliance. Additionally, both providers represent they are EU-US Privacy Shield Certified. HubSpot, AWS, and SurveyMonkey have published their GDPR compliance documents. You may read about their GDPR compliance and find each of their certifications below.

HubSpot represents that all sensitive interactions with the HubSpot products are encrypted in-transit with TLS 1.0, 1.1, or 1.2 and 2,048 bit keys or better and that it ensures stored data is encrypted at rest. The physical and virtualized hard drives used by HubSpot product server instances as well as long-term storage solutions use AES-256 encryption. Additionally, certain databases or field-level information is encrypted at rest, based on the sensitivity of the information. For instance, user passwords are hashed and certain email features work by providing an additional level of both at-rest and in-transit encryption. You may review HubSpot's certification and other documentation here:

HubSpot Privacy Shield Certification
HubSpot Security & Risk Management Program Overview

With regard to AWS, we are informed that in early 2018, AWS completed a GDPR service readiness audit. They represent that their security and compliance experts confirmed that AWS has in place effective technical and organizational measures for data processors to secure personal data in accordance with the GDPR. On 13 February 2017, AWS declared that Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail, and Amazon Elastic Block Store (Amazon EBS) are fully compliant with the CISPE Code of Conduct for Cloud Infrastructure Service Providers. AWS is also EU-US Privacy Shield certified. You may review their certification and other documentation here:

AWS Privacy Shield Certification
AWS Privacy Shield Framework
AWS GDPR Center
AWS GDPR Blog

SurveyMonkey stores European customer data on its servers in the US. They also provide customer support services from their US, European, Australian, and Canadian offices.

US Offices
- San Mateo, California
- Portland, Oregon
- Seattle, Washington

Ireland
- Dublin, Ireland

Canada
- Ottawa, Canada

Australia
- Sydney, Australia

SurveyMonkey represents that their information systems and technical infrastructure are hosted within SOC 2 accredited data centers. Physical security controls at their data centers include 24x7 monitoring, cameras, visitor logs, entry requirements, and dedicated cages for SurveyMonkey hardware. They further represent that they encrypt data in transit using secure TLS cryptographic protocols and that SurveyMonkey data is also encrypted at rest. We are also informed that SurveyMonkey is EU-US Privacy Shield certified. You may review their certification and other documentation here:

SurveyMonkey Privacy Shield Certification
SurveyMonkey Data Transfers
SurveyMonkey Security Statement

Additionally, we will provide information on a data subject where we are required to do so by law. Examples are complying with a court order or a lawful request by a public authority.

3.7 What is the legal basis for processing the data?

Each recipient of marketing communications will have first voluntarily opted in and requested that their private information be used to provide such information and content. Each recipient will find it just as easy to opt-out anytime they wish by visiting a link provided in each marketing communication received.

3.8 How long will the data be stored?

Data will be stored for the duration of the data subject's request to receive communications and/or subscriptions. We will send annual opt-in renewals to ensure the data subject's preferences are current. Once the data is in our system, it will be kept for the necessity of communicating with the data subject as requested. Once a request and/or subscription is terminated or the data subject opts out of receiving our communications, we will only keep data for as long as it is necessary to process the termination. If a data subject requests their information be deleted from our records, we will honor that request within the timeframe allowed by the GDPR and will pass the request along to our processors so that they may comply within the appropriate timeframe, as well. We cannot determine with any certainty how long a business relationship will last, how long a contact will remain our contact, or how many times a request and/or subscription with us will be renewed. However, we will conduct annual audits of data in storage to search for data able to be removed and deleted.

3.9 Do we use automated decision making or profiling?

We have lead nurturing workflows set up on our websites in which we automatically send relevant content to contacts based upon other content they have expressed interest in.

3.10 What rights do data subjects have?

Individual data subjects who receive our marketing communications may assert the following rights:

To receive certain information on the collection of personal data;
To access his/her personal data;
To rectify inaccurate personal data;
To be forgotten;
To restrict the processing of his/her data;
To transfer data from one organization to another;
To object to direct marketing; and
To object to automated decision making or profiling.

We will assist data subjects in exercising the rights listed above when data subjects assert their rights under GDPR.

4.0 Complaints Procedure

In the event of an infringement, should a data subject wish to lodge a complaint with regard to our company's control or processing of the information, they may do so with the supervisory authority of the Member State where they reside.

5.0 Training Policy

Key employees and decision makers across our business are aware of and trained on the GDPR so that they can consider how to ensure compliance and appropriately allocate resources. Staff training is conducted so that employees are aware of the main effects of the GDPR on their work.

6.0 Third Party Processors

We ensure our data processing vendors meet the requirements of the GDPR. At present, the following is a list of the third parties we contract with and a link to their GDPR compliance documents:

- Amazon Web Service GDPR Compliance Documents:
  Data Privacy
  GDPR Center
  AWS Security Blog

- HubSpot Info:
  HubSpot Privacy Policy
  HubSpot Data Processing Agreement
  The GDPR & HubSpot

- SurveyMonkey:
  Privacy Policy
  Commitment to GDPR Compliance
  GDPR White Paper

7.0 Data Protection Auditing Policy

We have conducted a comprehensive review and will perform quarterly reviews of all personal data we hold, whether it relates to current or past employees, marketing communications contacts, or other third parties. These reviews of personal data include examining:

Why are we holding it?
How did we obtain it?
Why was it originally gathered?
How long will we retain it?
How secure is it, both in terms of encryption and accessibility?
Do we ever share it with third parties and on what basis might we do so?

We will not keep personal data of individual data subjects longer than is necessary for the purpose for which it was obtained and processed.

8.0 Data Access Procedures

Data subjects can exercise their rights by contacting us at GDPR@adec-innovations.com. We will make every effort to respond within the timeframe required by the GDPR or we will notify the data subject why we cannot. Any information we provide will be in a machine-readable format free of charge.

9.0 Data Security Procedures

Should a data security breach occur, if the risk to rights and freedoms of data subjects is likely, we will notify the Data Protection Commissioner (DPC) within 72 hours of becoming aware of the breach. If such a notice is necessitated, it will include the following information:

The nature of the data breach including, where possible, the categories and approximate number of individuals and personal data records concerned;
The name and contact details of the DPO or other contact within the organization;
The likely consequences of the breach;
The measures taken or proposed to address the breach, including measures to mitigate possible adverse effects.

We will notify the data subjects themselves if there is a high risk to the data protection rights of individuals affected and will assist them in preparing the notice in the clear, plain language required by the GDPR.

10.0 Data Protection Impact Assessment

We will perform a Data Protection Impact Assessment (DPIA) each time a new type of processing or collection are contemplated which will help us determine if it will constitute a high risk to data subjects' private information and enable us to make the appropriate decisions and safeguards regarding that processing or collecting activity.

If you are also a client and use our platform or any of our applications, please see our European Customer policies and procedures.

These policies and procedures are effective 25 May 2018. Dates of revisions will be noted here as they become effective.