ADEC INNOVATIONS
ESG SOLUTIONS

FOR OUR SOFTWARE CUSTOMERS IN EUROPE:

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 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

ADEC Innovations includes the following business entities:

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

ADEC Innovations Ltd., a limited liability company registered in Bermuda.

ADEC Solutions UK, Ltd., a limited liability company registered in England.

AMDATEX Las Piñas Services, Inc. ("AMDATEX"), a corporation registered in the Philippines.

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.

ADEC Innovations is a dynamic network of applications, platforms, services, and solutions, architected within an integrated framework of corporate sustainability that ensures resource optimization, risk mitigation and long-term financial viability for its clients.

We do not collect personal data of individual data subjects.

We process data collected and controlled by our clients.

3.2 How we help clients comply with GDPR

When we receive requests for assistance from our clients, 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 client in a timely manner.

3.3 Who can our clients contact regarding our GDPR compliance?

For the convenience of our customers, 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 clients determine what data is entered into our system. Should an individual data subject not provide data to our clients, there would be no consequence to our business, platform, or software applications. However, once the data is in our system the removal of it may be detrimental to our legitimate business interests. Data storage is discussed further below in this policy.

The data input into our software applications enables the clients to effectively use our software applications and platform.

The purpose for processing the following data is to allow our clients to effectively use our software. Our client's data provides context so that they can make effective use of our software.

Our system contains the following categories of data to be used as described below:

Name - Used to identify a user within our software.

Identification number - Used to link the data subject with other third-party software tools such as reporting and business intelligence products.

Online identifier - Used to allow data subjects to log into our applications and they are comprised exclusively of usernames.

Email address - Used to send messages to data subjects. Email addresses can also be used as usernames within our software.

Title - Used for messages to data subjects as well as indicating their organizational role.

Telephone Number - Stored in our software to allow suppliers in a data subject's supply chain to contact them.

3.5 To whom the data will 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:

Customer Success Team – Located in Irvine, California; and Sacramento, California, U.S.A.

Customer Support Team – Located in Ayala Alabang, Muntinlupa, Metro Manila, Philippines

Data Bureau Team – Located in Ayala Alabang, Muntinlupa, Metro Manila, Philippines

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

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

Customer Success Team – Reviews the data, populates certain data, and provides our Data Bureau Team guidance, if necessary.

Customer Support Team – Reviews data in order to resolve an issue at the customer's request.

Data Bureau Team – Uploads data on behalf of the customer.

Product Management Team – Reviews the data, populates certain data, and provides our Data Bureau Team guidance, if necessary.

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 our customers.

3.6 Will data leave the European Economic Area?

Data input into our software applications will be transferred outside the European Economic Area. Data will be transferred using Amazon Web Services (AWS) and will be stored by AWS in their facility in Portland, Oregon, U.S.A.

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

Also, AWS has published its GDPR compliance documents and you may review them here.

AWS GDPR Center
AWS GDPR Blog

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 client pays a fee and enters into a contract and/or subscription with us to provide them access to our software applications. In order to fulfill contractual obligations with our clients, we must store the data they enter and make it available to them in the software.

3.8 How long will the data be stored?

Data will be stored for the duration of the contract and/or subscription with each client and all subsequent renewals. Once the data is in our system, it will be kept for the necessity of performance of the contract or subscription with the client and it may become a necessary legitimate business interest for the adequate function of the system to retain such data for a period of time after the business relationship has concluded. Once a contract and/or subscription is terminated, we will only keep data that is necessary for the legitimate interests of our business in the function of the software applications and only for as long as that data is necessary. We cannot determine with any certainty how long a business relationship will last, how long a client will remain our client, or how many times a contract and/or subscription with us will be renewed. However, while each business relationship is different, a typical contract and/or subscription term is one to three years. 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?

Not at this time.

3.10 What rights do data subjects have?

We do not do business with individual data subjects. We do business with other business entities. We do not control or collect data of individual data subjects. We process the data of our corporate clients which includes information regarding individual data subjects. Individual data subjects may assert the following rights to our clients:

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.

As a processor of information, we will assist our clients in complying when data subjects assert their rights under GDPR.

4.0 Complaints Procedure

In the event of an infringement, should a client's data subject wish to lodge a complaint with regard to our company's processing of the information controlled by our client, 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
- OutSystems

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 former customers, current or past employees, unsuccessful job candidates 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 processed.

8.0 Data Access Procedures

It is our belief that our clients own their data. In addition to assisting with GDPR compliance of our clients, at the end of a contract or the cancellation of a subscription, we will, upon request and where feasible, provide a client's corporate data to the client in a machine-readable format free of charge. To request our assistance with GDPR requests from data subjects or any other GDPR related questions, please contact us at GDPR@adec-innovations.com. We will make every effort to respond within the timeframe required by the GDPR or we will notify you that we need additional time and why. 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 our clients 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 receive marketing communications from us, please see our marketing policies and procedures.

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