



**Data Processing Agreement  
for all contracted Cloud Hosted  
Server, Remote Back-Up and  
EMIR Support & Maintenance Customers**

<b>Document Ref.</b>	
<b>Version:</b>	<b>1</b>
<b>Dated:</b>	<b>19 May 2018</b>

## 1 Parties to the Agreement

The Controller: Applicable to all contracted customers of Solutions In I.T. including EMIR Software users, Cloud Hosted Server clients and Remote Back-Up customers.

The Processor: Solutions In I.T. Limited, Harborough Innovation Centre, Airfield Business Park, Leicester Road, Market Harborough, Leicestershire. LE16 7WB. Company Number 4555311

## 2 Scope and Roles

- 2.1 This agreement applies to the processing of Personal Data, within the scope of the GDPR, by the Processor on behalf of the Controller.
- 2.2 For purposes of this agreement, <<controllers, as listed in section 1>> and Solutions In I.T. agree that <<controllers, as listed in section 1>> is the Controller of the Personal Data and Solutions In I.T. is the Processor of such data. In the case where <<controllers, as listed in section 1>> acts as a Processor of Personal Data on behalf of a third party, **Solutions In I.T.** shall be deemed to be a Sub-Processor.
- 2.3 These Terms do not apply where Solutions In I.T. is a Controller of Personal Data.

### 3 Definitions

3.1 For the purposes of this Agreement, the following definitions shall apply:

Agreement	This data processing agreement
GDPR	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Personal Data	means that data, meeting the definition of “personal data” as defined in Article 4 of the GDPR, that is provided by <<controllers, as listed in section 1>> to Solutions In I.T. in order to perform the processing as defined in Schedule 1 of this Agreement.
Sub-Processor	means a natural or legal person, public authority, agency or body other than the data subject, Controller and Processor who, under the direct authority of the Processor, are authorised to process Personal Data for which <<controllers, as listed in section 1>> is the Controller.

Terms used but not defined in this Data Processing Agreement (e.g., “processing”, “controller”, “processor”, “data subject”) shall have the same meaning as in Article 4 of the GDPR.

### 4 The Processing

4.1 The subject matter, duration, nature and purpose of the Processing, and the types of Personal Data and categories of data subjects shall be as defined in Schedule 1 of this Agreement.

### 5 Obligations and rights of the controller

5.1 Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that Processing is performed in accordance with the GDPR. Those measures shall be reviewed and updated where necessary.

- 5.2 Where proportionate in relation to Processing activities, the measures referred to in paragraph 5.1 shall include the implementation of appropriate data protection policies by the Controller.
- 5.3 The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data are not made accessible without the individual's intervention to an indefinite number of natural persons.

## **6 Obligations of the Processor**

6.1 The Processor shall:

- 6.1.1 process the Personal Data only on documented instructions from the Controller;
- 6.1.2 ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- 6.1.3 take all measures required pursuant to Article 32 of the GDPR, namely to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of natural persons including, as a minimum, the measures set out in Schedule 2 of this Agreement;
- 6.1.4 respect the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another Processor, namely that the Processor may not engage another Processor (Sub-Processor) without the prior authorisation of the Controller. Those Sub-Processors that are authorised by the Controller at the date of this agreement are listed in Schedule 3. In cases where another Processor is engaged, the Sub-Processor must be subject to the same contractual terms as described in this Agreement;
- 6.1.5 assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
- 6.1.6 assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, relating to security of Processing, Personal Data Breaches and data protection impact assessments;
- 6.1.7 at the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing, and

delete existing copies unless applicable law requires storage of the Personal Data;

- 6.1.8 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;

## **7 Duration and Applicable Law**

- 7.1 This Agreement shall continue in effect for so long as the Processor is processing Personal Data on behalf of the Controller.
- 7.2 This Agreement shall be governed by the laws of England and Wales and subject to the exclusive jurisdiction of the courts of England and Wales.

## 8 Signatures

### Controller

No signature is required for contracted Cloud Hosted Server and Remote Back-Up clients and/or where customers have a valid EMIR Support & Maintenance agreement. This agreement applies wherever there is an invoiced amount, that is paid, for such a service in the current period.

### Processor

Signed for and on behalf of Solutions In I.T.:

<b>Name</b>	Gary Downes
<b>Title</b>	Managing Director
<b>Date</b>	19 <sup>th</sup> May 2018

**SCHEDULE 1 – Description of the Processing**

<p><b>Subject matter and duration of the Processing</b></p>	<p>Solutions In I.T. supply services of support and require access to EMIR software for purposes of upgrade and maintenance. For this reason, they do need to access a client’s data using secure remote connection capability. As the length of time for each operation varies, Solutions In I.T. will keep the customer informed of each individual operation.</p>
<p><b>Nature and purpose of the Processing</b></p>	<p>Maintenance – Solutions In I.T. need to keep their EMIR Software application up-to-date and will periodically (with consent of the client) load new features and fixes using remote connection software.</p> <p>Support – From time-to-time, Solutions In I.T. will be required to access an EMIR system to educate and/or resolve reported or known issues. This will usually be at the users request.</p> <p>Cloud Hosted Servers – The support of cloud hosted servers is undertaken by Solutions In I.T. who may need to connect remotely to offer advice and make changes. Solutions In I.T. may refer issues to their designated provider, i-Dash Limited (sub-processor), who also may require access.</p> <p>Remote Cloud Back-Up – Solutions In I.T. use an automated, secure back-up procedure. They retain access to the control console of the back-up system to ensure that the correct information is collected and that the process actually takes place at the desired time.</p> <p>Our sub-processing partners as per Schedule 3 below may also require access depending on the product or service provided.</p> <p>No passwords or usernames are held by Solutions In I.T. and the user has the right to change entry information when the work has taken place.</p>
<p><b>Type of Personal Data and categories of data subjects</b></p>	<p>As Solutions In I.T. are the authors of the business system EMIR, they do come into contact with a wide range of data including customer &amp; supplier contact records, prospective client data and personnel &amp; HR.</p>

## **SCHEDULE 2 – Technical and Organisational Measures**

The following security measures shall be implemented by the Processor, as a minimum:

### **EMIR Software Customers**

Password & usernames – a system administration account is issued on the initial installation of the system with the recommendation for the client to change it to ensure internal security. This account requires our access for support purposes, so we must be informed of any changes to it when support is required. Any such system admin account passwords held by us, for such support purposes, are stored in a secure password management application accessible only to the required staff who are trained in their management of personal data.

### **Cloud Hosted Server and Remote Back-Up**

Cloud servers are stored in a 'blue-chip', secure data centre with physical and software level security and intelligent firewall devices. Backup services use encrypted data both in transit and at rest. Cloud server data is replicated to a separate cloud server site. All cloud servers are continually patched to the latest o/s levels with anti-virus and anti-malware functionality as standard. All such cloud service security measures are managed by our sub-processing partners, i-Dash Ltd. No user-level passwords are stored by us and so passwords must be reset if lost or forgotten. Admin level accounts, required for management and support purposes are stored in a secure password management application accessible only to the required staff who are trained in their management of personal data.

### **PC Supply**

Any desktop PC's and laptop devices used by Solutions In I.T. are patched with the latest versions of their operating systems, anti-virus and malware, as required.

### **Our Offices and Servers**

Our office is protected by both building level and room level alarms and doors and locks are of the required BS standard. We are on the 2<sup>nd</sup> floor of a shared office building. In a disaster recovery situation, we can work from home as all data is available on our cloud servers, which can be accessed from any location or machine with suitable usernames and passwords. So, as long as we have access to the internet, we can function. Again, if the office loses internet connectivity, staff can work from home and we can also use USB dongles to ensure we can access via 4G, if absolutely necessary to provide our services. Our servers and data are backed up daily to a full image solution, such that a new server can be built quickly in the event of a fatal server incident. Any newly commissioned server can be reinstalled at one of two data centres operated by our partners.



### **SCHEDULE 3 – Sub-Processors**

As at the date of this agreement, the following Sub-Processors have been notified by the Processor to the Controller with respect to the Processing:

#### **3.1 Sub-processors for Cloud services and remote backup services.**

i-dash Ltd  
105 Great North Road  
St Neots  
PE19 8EL

#### **3.2 Sub-processors for all EMIR software products**

FHG Software Ltd  
Unit 2, Shield House  
Elizabeth Way  
Harlow  
Essex  
CM19 5AR

#### **3.3 Sub-processors for the EMIR “Smart Site” product**

Swipe and Tap Ltd  
Dock 210  
75 Exploration Drive  
Leicester  
LE4 5NU

#### **3.4 Sub-processors for the EMIR “Workshop Routing” product.**

Confluent.  
405 Golfway Drive West  
Suite 103-D  
ST Augustine  
Florida  
32095 US