Gremon Systems Zrt.

PRIVACY NOTICE FOR CROP MONITOR AND FORECASTER CUSTOMERS

PRIVACY NOTICE FOR CROP MONITOR AND FORECASTER CUSTOMERS

Gremon Systems Zrt. built the Crop Monitor App as a Free App. The App is just an additional tool for a SERVICE supplied by Gremon Systems Zrt. which must be ordered and paid first in order to be able to use the App.

Supplier as a data controller is committed to protecting the privacy of its Customers. This Policy applies to the processing of personal data of natural person end user Customers of Supplier (hereafter referred to as '**Data Subject**'). Supplier handles personal data with utmost care and in accordance with Supplier's obligations under applicable data protection and privacy laws. This privacy policy ('Notice') describes for what purposes and how Supplier obtains and processes personal data when providing Services under the Terms of Service.

Purposes of data processing include

- Entering into a contact with the Customer for providing the Services; setting up and maintaining Products and Services;
- Education and training to Data Subjects;
- Development of Products and Services
- Communications and direct marketing;
- Handling of complaints and Customer inquiries;
- Enforcement of legal claims;
- Compliance with legal and other regulatory requirements.

The Notice is structured as follows:

WHO IS THE CONTROLLER

The data controller is Supplier that is GREMON SYSTEMS Zrt. (registered office: Hungary, H-6721 Szeged, Dugonics utca 42.; registration number: 06-10-000460).

THE PURPOSES OF DATA PROCESSING

Supplier processes Personal Data of Customers in order to take steps to enter into a contract with the Data Subject and to provide the Services to such end Customers under the Terms of Service, including

- Entering into a contact with the Customer for providing the Services; setting up and maintaining Products and Services, including technical support, providing software upgrades; Billing, invoicing and collection of fees and payments
- Education and training to Data Subjects;
- Development of Products and Services, including conducting market research to improve Services and to develop new products and services according to the needs of Customers.
- Communications, including notifications and updates on the Products and Services, and direct marketing via e-mail on the Products and Services if the Customer opts in to such communications;
- Handling of complaints and Customer inquiries;
- Enforcement of legal claims;
- Compliance with legal and other requirements, including record-keeping and reporting obligations, compliance with government inspections and other requests from public authorities, responding to legal processes and disclosure of Personal Data where required to do so by law enforcement agencies.

THE LEGAL BASES OF DATA PROCESSING

- **Contract:** The processing of Personal Data under this Notice is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract and necessary for Supplier to perform obligations under the Terms of Service pursuant to Article 6 (1) b) of the GDPR.

- **Consent:** If a Data Subject opts-in to direct marketing communications via e-mail or postal mail, then data processing will be based on Article 6 (1) a) of the GDPR. The Customer may at any time withdraw its consent. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

- **Legal obligation:** Supplier will process Personal Data under Article 6 (1) (c) in order to comply with its obligations to billing, accounting and reporting to the Tax Administration under Hungarian laws.

- **Legitimate interests:** Supplier may also process Personal Data pursuant under Article 6 (1) (f) of the GDPR for the enforcement of its claims (if any) and to monitor compliance of Data Subjects with the Terms of Service in order to prevent or avert misuse of the Services; or to secure the quality of Personal Data it processes. Supplier may also consult public registers (company register, register of private entrepreneurs) in order to secure the quality (validity and accuracy) of Personal Data. Supplier established that it has a prevailing legitimate interest to process personal data for these purposes.

PERSONAL DATA SUPPLIER COLLECTS

Supplier uses certain basic Personal Data to be able to deliver Products or Services to private individuals. Supplier collects and uses the following Personal Data categories from its natural person end Customers:

- Name - necessary for the identification of the Data Subject
- Address - necessary for the identification of the Data Subject
- Tax ID- necessary for the handling of payments and billing
- User name - necessary for the provision of the Services and to identify the Data Subject

- Password; - necessary for the provision of the Services and to identify the Data Subject
- E-mail address - necessary for the communication with the Data Subject;
- Language preferences - necessary for the communication with the Data Subject
- Location data (GPS coordinates) - necessary for Service provision to the Data Subject
- Time Zone - - necessary for Service provision to the Data Subject
- Customer Data; - necessary for Service provision to the Data Subject
- Payment and Billing Details- - necessary for the handling of payments and billing
- Data Relating to Security Incidents (time and description of the incident)- - necessary for the handling of or future prevention of such incidents.
- Pictures – necessary for Service provision to the Data Subject.
- Voice massages - necessary for Service provision to the Data Subject.

The provision of Personal Data is voluntary. If the Customer does not provide the Personal Data indicated above, the Supplier may not be able to provide the Services under the Terms of Service.

DATA RECIPIENTS

Supplier has measures in place securing that only persons within the Supplier's organization with a "need to know" may have access to the end user Customer's Personal Data. Supplier may, in the course of the provision of the Services utilize the services of various data processors and external service providers to handle and process Personal data for specific purposes, on behalf of and in accordance with its instructions. Personal Data may be provided to parties that are located outside the European Economic Area ("EEA"). In such cases, Supplier will ensure that the Personal Data is subject to measures that provide an equivalent level of protection as provided by data privacy laws in the EU (such as the EU General Data Protection Regulation; GDPR).

The app does use third party services that may collect information used to identify you.
Link to privacy policy of third party service providers used by the app Google Play Services

Amazon Web Services, Inc. (410 Terry Avenue North, Seattle, Washington- 98109-5210, hereafter "AWS") as a cloud provider acting as a data processor in relation to the storage and retention of Personal Data. Data transfer to Amazon, Inc. involves data transfer to the United States. AWS is certified under the EU-US Privacy Shield. View the certification at https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4

LOG DATA

We want to inform you that whenever you use our Service, in a case of an error in the app we collect data and information (through third party products) on your phone called Log Data. This Log Data may include information such as your device Internet Protocol (“IP”) address, device name, operating system version, the configuration of the app when utilizing our Service, the time and date of your use of the Service, and other statistics.

COOKIES

Cookies are files with a small amount of data that are commonly used as anonymous unique identifiers. These are sent to your browser from the websites that you visit and are stored on your device's internal memory.
This Service does not use these “cookies” explicitly. However, the app may use third party code and libraries that use “cookies” to collect information and improve their services. You have the option to either accept or refuse these cookies and know when a cookie is being sent to your device. If you choose to refuse our cookies, you may not be able to use some portions of this Service.

CHILDREN’S PRIVACY

These Services do not address anyone under the age of 13. We do not knowingly collect personally identifiable information from children under 13. In the case we discover that a child under 13 has provided us with personal information, we immediately delete this from our servers. If you are a parent or guardian and you are aware that your child has provided us with personal information, please contact us so that we will be able to do necessary actions.

DATA RETENTION

Personal Data will not be kept in a form that allows the Data Subject to be identified for any longer than is reasonably considered necessary by the Supplier for achieving the purposes for which it was collected or processed. Personal Data will, in any case, be retained for the duration of the Service provision as well as thereafter as long as there are statutory retention obligations (eight years under the Hungarian Act on Accounting) or potential claims resulting from the Data Subjects use of the Services are not yet time-barred under the Hungarian Civil Code that is at least five years from the termination of the Services provision. We will not process Personal Data with consent after the period of five years following the recordal of such consent. Any other Personal Data will in principle be deleted no more than 2 years after the last interaction and business contact with the Data Subject. The Personal Data will be removed from our records or properly anonymized when it is no longer needed.

DATA SECURITY

Supplier will take appropriate measures to protect Personal Data that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of Personal Data.

Supplier will implement necessary organizational and technical measures to ensure the ongoing confidentiality, integrity, availability and resiliency of the Services and systems processing personal data.

RIGHTS AND REMEDIES

Pursuant to the applicable data protection law the Data Subject has the right (i) to request access to your personal data, (ii) to request rectification of Personal Data, (iii) to request erasure of Personal Data, (iv) to request restriction of processing of Personal Data, (v) to request data portability, (vi) to object to the processing of Personal Data (including objection to profiling; also other rights in connection with automated decision-making).

To the extent the EU General Data Protection Regulation applies:

(i) Right of access

The Data Subject has the right to obtain from Supplier confirmation as to whether or not Personal Data concerning the Data Subject is processed, and, where that is the case, to request access to the Personal Data. The access information includes – inter alia – the purposes of the processing, the categories of Personal Data concerned, and the recipients or categories of recipient to whom the Personal Data have been or will be disclosed. The Data Subject has the right to obtain a copy of the Personal Data undergoing processing. For further copies requested by the Data Subject, Supplier may charge a reasonable fee based on administrative costs.

(ii) Right to rectification

Data Subjects have the right to obtain from Supplier the rectification of inaccurate Personal Data concerning the Data Subject. Depending on the purposes of the processing, Data Subjects may have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

(iii) Right to erasure (right to be forgotten)

Under certain circumstances Data Subjects may have the right to obtain from Supplier the erasure of Personal Data concerning them, and Supplier may be obliged to erase such Personal Data.

(iv) Right to restriction of processing

Under certain circumstances the Data Subject has the right to obtain from Supplier the restriction of processing of Personal Data. In this case the respective data will be marked and may only be processed by Supplier for limited purposes.

(v) Right to data portability

The Data Subject has the right to receive the Personal Data concerning him/her, which the Data Subject have provided to Supplier, in a structured, commonly used and machine-readable format and the Data Subject may have the right to transmit those data to another entity without hindrance from Supplier.

(vi) Right to object:

Data Subjects have right to object, on grounds relating to the relevant Data Subject's particular situation, at any time to the processing of Personal Data by the Supplier when Supplier can be required to no longer process Personal Data. If the Data Subject has a right to object and he/she exercises this right, and the objection is substantiated, his/her Personal Data will no longer be processed for such purposes by the Supplier. Exercising this right will not incur any costs. Such a right to object may not exist, in particular, if the processing of Personal Data is necessary to take steps prior to entering into a contract or to perform a contract already concluded with the Data Subject. Moreover, if the Data Subject's Personal Data is processed for direct marketing purposes, the Customer has the right to object at any time to the processing of Personal Data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing. In this case the relevant Data Subject's Personal Data will no longer be processed for such purposes by Supplier.

(vii)
Moreover, if the Data Subject's Personal Data is processed for direct marketing purposes, you have the right to object at any time to the processing of Personal Data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing. In this case the relevant Data Subject's Personal Data will no longer be processed for such purposes by Supplier.

Furthermore, under certain circumstances in case of automated individual decision-making, the Data Subject has the right to obtain human intervention, to express his/her point of view and to contest the decision.

RIGHT TO COMPLAINT
The Data Subject have the right to lodge a complaint with the competent data protection supervisory authority. If the Data Subject believes that his/her rights have been infringed, the Data Subject may contact the Hungarian National Data Protection and Freedom of Information Agency (1024 Budapest, Szilágyi Erzsébet fasor 22/C.; telephone: +36-1-391-1400, telefax: +36-1-391-1410, e-mail: ügyfelszolgalat@naih.hu).

HOW TO CONTACT US
The contact information for data protection inquiries and requests by Data Subjects is:

GREMON SYSTEMS Zrt.
info@gremonsystems.com.
+36-70-310-6609

SCHEDULE 3

PERSONAL DATA PROCESSING AGREEMENT

This Personal Data Processing Agreement ("PDPA") is entered into by and between the Customer as defined in the Terms of Service and Supplier (Gremon Systems Zrt) and governs the processing of Personal Data by Supplier on behalf of the Customer. Unless otherwise indicated in this PDPA, the definitions in Clause 2 of the Terms of Service shall apply to this PDPA.

1. Definitions

For the purposes of this PDPA:

"**Applicable Data Protection Law**"	shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to Controller and Processor; the term Applicable Data Protection Law shall encompass the GDPR once it comes into effect on May 25, 2018;
"Controller"	shall mean the Customer under the Terms of Service who determines as a natural or legal person alone or jointly with others the purposes and means of the Processing of Personal Data;
"PDPA"	shall mean the Data Processor Agreement in Schedule 3 of these Terms of Service
"General Data Protection Regulation" or "GDPR"	**shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data which will come into effect on May 25, 2018;**
"Member State"	**shall mean a country belonging to the European Union;**
"Personal Data"	**shall have the meaning defined in the Terms of Service.**
"**Personal Data Breach**"	**shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data transmitted, stored or otherwise Processed;**
"Process/Processing"	**shall mean 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;**
"Processor"	**shall mean GREMON SYSTEMS Zrt. (registered office: Hungary, 6721 Szeged, Dugonics utca 42.; registration number: 06-10-000460; EU VAT number: HU24780593) as Supplier who Processes Personal Data on behalf of Controller;**
"Special Categories of Data"	**shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data, biometric data Processed for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation;**

"Sub processor"	**shall mean any data processor engaged by Supplier who agrees to receive from Supplier Personal Data exclusively intended for Processing activities to be carried out on behalf of Controller in accordance with its instructions, the terms of this PDPA and the terms of the written subcontract;**
"Supervisory Authority"	**shall mean an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR; and**
"Technical and Organizational Security Measures"	**shall mean those measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.**

2. Details of the Processing

The details of the Processing operation provided by Supplier to Controller as a commissioned data processor (e.g., the subject-matter of the Processing, the nature and purpose of the Processing, the type of personal data and categories of data subjects) are specified in Annex 1 to this PDPA.

3. Rights and Obligations of Controller

Controller remains the responsible data controller for the Processing of the Personal Data as instructed to Supplier based on the Terms of Service, this PDPA and as otherwise instructed. Controller has instructed and throughout the duration of the commissioned data processing will instruct Supplier to Process the Personal Data only on Controller's behalf and in accordance with the Applicable Data Protection Law, the Terms of Service, this PDPA and Controller's instructions. Controller is entitled and obliged to instruct Supplier in connection with the Processing of the Personal Data, generally or in the individual case. Instructions may also relate to the correction, deletion, blocking of the Personal Data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by Controller in writing without delay. To the extent that the implementation of an instruction results in costs for Supplier, Supplier will first inform Controller about such costs. Only after Controller's confirmation to bear such costs for the implementation of an instruction, Supplier is required to implement such instruction.

4. Obligations of Supplier

Supplier shall:

(a) Process the Personal Data only as instructed by Controller and on Controller's behalf; such instruction are provided in the Terms of Service, this PDPA and otherwise in documented form as specified in Sec. 3 above; such obligation to follow Controller's instruction also applies to the transfer of the Personal Data to a third country or an international organization.

(b) inform Controller promptly if Supplier cannot comply with any instructions from Controller for whatever reasons, in which case Controller is entitled to suspend the transfer of Personal Data and/or terminate this PDPA and/or the Terms of Service.

(c) ensure that persons authorized by Processors to Process the Personal Data on behalf of Controller have committed themselves to confidentiality or are under an appropriate obligation of confidentiality and that such persons that have access to the Personal Data Process such Personal Data in compliance with Controller's instructions.

(d) implement the Technical and Organizational Security Measures which will meet the requirements of the Applicable Data Protection Law as further specified in Annex 2 before Processing of the Personal

Data and ensure to provide sufficient guarantees to Controller on such Technical and Organizational Security Measures.

(e) assist Controller by appropriate Technical and Organizational Measures, insofar as this is feasible, for the fulfilment of Controller's obligation to respond to requests for exercising the Data Subjects rights concerning information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making; to the extent such feasible Technical and Organizational Measures require changes or amendments to the Technical and Organizational Measures specified in Annex 2, Processor will advise Controller on the costs to implement such additional or amended Technical and Organizational Measures. Once Controller has confirmed to bear such costs, Processor will implement such additional or amended Technical and Organizational Measures to assist Controller to respond to Data Subject's requests.

(f) make available to Controller all information necessary to demonstrate compliance with the obligations laid down in this PDPA and in Art. 28 GDPR and allow for and contribute to audits, including inspections conducted by Controller or another auditor mandated by Controller. Controller is aware that any in-person on-site audits may significantly disturb Supplier’s business operations and may entail high expenditure in terms of cost and time. Hence, Controller may only carry out an in-person on-site audit if Customer reimburses Supplier for any costs and expenditures incurred by Supplier due to the business operation disturbance.

(g) notify Controller without undue delay:
  (i) about any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
  (ii) about any complaints and requests received directly from the Data Subjects (e.g., regarding access, rectification, erasure, restriction of Processing, data portability, objection to Processing of data, automated decision-making) without responding to that request, unless it has been otherwise authorized to do so;
  (iii) if Supplier is required pursuant to EU or Member State law to which Supplier is subject to Process the Personal Data beyond the instructions from Controller, before carrying out such Processing beyond the instruction, unless that EU or Member State law prohibits such information on important grounds of public interest; such notification shall specify the legal requirement under such EU or Member State law; and
  (iv) if, in Supplier's opinion, an instruction infringes the Applicable Data Protection Law; upon providing such notification, Supplier shall not be obliged to follow the instruction, unless and until Controller has confirmed or changed it.
  (v) after Supplier becomes aware of a Personal Data Breach at Supplier or its Sub processors. In case of such Personal Data Breach, Supplier will assist Controller with Controller's obligation und Applicable Data Protection Law to inform the data subjects and the Supervisory Authorities, as applicable, and to document the Personal Data Breach.

(h) assist Controller with any Data Protection Impact Assessment as required by Art. 35 of the GDPR that relates to the Services provided by Supplier to Controller and the Personal Data Processed on behalf of Controller.

(i) deal with all inquiries from Controller relating to its Processing of the Personal Data subject to the Processing (e.g., to enable Controller to respond to complaints or requests from Data Subjects in a timely manner) and abide by the advice of the Supervisory Authority with regard to the Processing of the data transferred.

(j) to the extent that Supplier is required and requested to correct, erase and/or block Personal Data Processed under this PDPA, Supplier will do so without undue delay. If and to the extent that Personal Data cannot be erased due to statutory retention requirements, Supplier shall, in lieu of erasing the relevant Personal Data, be obliged to restrict further Processing and/or use of Personal Data (hereinafter referred to as "blocking"). If Supplier is subject to such blocking obligation, Supplier

shall completely and irrevocably erase the relevant Personal Data on the last day of the calendar year during which the retention term ends.

6. Sub processing

(a) Controller authorizes the use of Sub processors engaged by Processor for the provision of the Services. Controller approves the following Sub processors:

Name	Address	Purpose of use
Amazon Web Services, Inc.	410 Terry Avenue North, Seattle, Washington-98109-5210	cloud hosting services; AWS is certified under the EU-US Privacy Shield. View the certification at https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Office 365, Sharepoint for storage internal company data, includes CRM and customer data
Domainsector Kft.	2013 Pomáz, Mikszáth Kálmán utca 36/4., Hungary	Domain names
BlazeArts Kft	6090 Kunszentmiklós, Damjanich utca 36. 1. em. 8.	Aruba cloud hosting service;
rEvolution Kft.	1133 Budapest, Váci út 76. 7. em.	DEEP ERP system for invoicing and stock keeping and other resource planning

(b) In case Processor intends to engage new or additional Sub processors, Processor shall inform Controller of any intended changes concerning the addition or replacement of any Sub processor ("**Sub processor Notice**"). If Controller has a reasonable basis to object to the use of any such new or additional Sub processor, Controller shall notify Processor promptly in writing within 14 days after receipt of the Sub processor Notice. In the event Controller objects to a new or additional Sub processor, and that objection is not unreasonable, Processor will use reasonable efforts to make available to Controller a change in the Services or recommend a commercially reasonable change to Controller's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new or additional Sub processor without unreasonably burdening Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Controller may terminate the effected part of the Terms of Service with respect only to those Services which cannot be provided by Processor without the use of the objected-to new or additional Sub processor by providing written notice to Processor.

(c) Processor shall impose the same data protection obligation as set out in this PDPA on any Sub processor by contract. The contract between Processor and Sub processor shall provide sufficient guarantees to implement the Technical and Organizational Security Measures as specified in Annex 2, to the extent such Technical and Organizational Security Measures are relevant for the services provided by Sub processor.

(d) Processor shall choose Sub processor diligently.

(e) In case any such Sub processor is located outside the EU/EEA in a country that is not recognized as providing an adequate level of data protection, Processor will upon Controller's written request enter with the relevant Sub processor on Controller's behalf (in the name of Controller) into EC

Model Clauses (Controller to Processor). In this case, Controller instructs and authorizes Processor to instruct Sub processors in Controller's name and to make use of all Controller's rights vis-à-vis the Sub processors based on the EC Model Clauses.

(f) Processor shall remain fully liable to Controller for the performance of Sub processor's obligations, should Sub processor fail to fulfil its obligations. However, Processor shall not be liable for damages and claims that ensue from Controller's instructions to Sub processors.

7. Limitation of liability

Any liability arising out of or in connection with this PDPA shall follow, and be exclusively governed by, the liability provisions set forth in, or otherwise applicable to, the Terms of Service. Therefore, and for the purpose of calculating liability caps and/or determining the application of other limitations on liability, any liability occurring under this PDPA shall be deemed to occur under the relevant Terms of Service.

8. Duration and termination

(a) The term of this PDPA is identical with the term of the relevant Terms of Service. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the relevant Terms of Service.

(b) Supplier shall, at the choice of Controller, delete or return all Personal Data to Controller after the end of the provision of Services, and delete any existing copies unless EU or Member State law requires Supplier to retain such Personal Data.

9. Miscellaneous

(a) In the event of inconsistencies between the provisions of this PDPA and any other agreements between the Parties, the provisions of this PDPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this PDPA shall prevail.

(b) Should any provision of this PDPA be invalid or unenforceable, then the remainder of this PDPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this PDPA contains any omission.

(c) This PDPA shall be governed by the same law as the Terms of Service except to the extent that mandatory Applicable Data Protection Law applies.

Annex 1 to the PDPA

Categories Data Subjects
The Personal Data transferred concern the following categories of Data Subjects:

- Authorized Users of the Customer.

Subject-matter of the processing
Provision of the Services as defined in the Terms of Service.

Nature and purpose of the processing
Processor Processes the Personal Data of the Data Subjects on behalf of Controller in order to provide the Services that is used by Controller to enable Authorized Users to use the Services as further described in the Terms of Service.

Type of personal data
The Personal Data Processed by Processor on behalf of Controller concern the following categories of personal data:
Personal Data of Authorized Users related to the Services, such as

- Name
- Address
- Tax ID
- User name
- Password;
- E-mail address
- Language preferences
- Location data (GPS coordinates)
- Time Zone
- Customer Data;
- Payment Details.
- Pictures.
- Voice massages.

Special Categories of Data
The transfer of Special Categories of Data is not anticipated.

Annex 2 to the PDPA

Description of the Technical and Organizational Security Measures implemented by Service Provider in accordance with Applicable Data Protection Law:

This Annex describes the Technical and Organizational Security Measures and procedures that Service Provider shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtained.

General information security and data protection strategies

The following measures shall be implemented to address general information security and data protection strategies:

a) performing information security and enterprise risk assessments, vulnerability scans, risk trend analysis, self-assessments, internal audits on a regular basis to identify security risks and mitigation strategies;
b) providing information security and data protection awareness training as part of the information security and data protection program for new hires and for exiting employees on an annual basis; monitoring of completion rate;
c) having available a system description for all in scope systems; documentation is maintained and accessible to all employees requiring access to such documents;
d) a formal process of documentation, specification, testing, quality control, communication and managed implementation (including back-out plans) whenever new systems are implemented or existing systems are changed (a verification testing is performed whenever major changes to the systems take place and such verification testing also includes security testing of the changes to the system); approvals are obtained prior to development, testing, and implementation for production;
e) description of the organization structure, system support functions, processes, organizational roles, responsibilities and organizational structure, including reporting relationships is regularly evaluated;
f) roles and responsibilities are defined, regularly reviewed, updated and communicated.

Organization of information security

The following measures shall be implemented to address a management structure and mechanism for coordinating information security and data protection activities:

a) clearly defined information security and data protection responsibilities due to policies;
b) all employees have been committed to keeping personal data confidential and not to disclosing personal data to any individual who does not have a need to know or is otherwise unauthorized, and have been made aware of the potential consequences in case of a violation of this commitment;

Access Control of Processing Areas

Service Provider implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are Processed. This is accomplished by:

- establishing security areas;
- securing the data processing equipment;
- establishing access authorizations for staff and third parties, including the respective documentation;
- access to data centres is logged and monitored; and
- data centres are protected by appropriate security measures.

Access Control to Data Processing Systems

Service Provider implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- identification of the terminal and/or the terminal user to the data importer systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);

- issuing and safeguarding of identification codes;
- staff policies and training in respect of each staff access rights to personal data (if any), informing staff about their obligations;
- access to data is logged and monitored.

Access Control to Use Specific Areas of Data Processing Systems

Service Provider commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- staff policies and training in respect of each staff member's access rights to the personal data;
- allocation of individual user accounts;
- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data to only authorized persons;
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

Availability Control

Service Provider implements suitable measures to ensure that personal data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy;
- any detected security incident is recorded, alongside the followed data recovery procedures, and the identification of the person who carried them out.

Transmission Control

Service Provider implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of appropriate firewall and encryption technologies;
- as far as possible, all data transmissions are logged and monitored; and
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

Input Control

Service Provider implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel;
- utilization of user codes (passwords);
- all users who have access to personal data shall reset their passwords as specified in the relevant password policy; and
- areas housing the computer hardware and related equipment are capable of being locked.

System Administrators

Service Provider implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for a reasonable period; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

Separation of Processing for Different Purposes

Service Provider implements suitable measures to ensure that data collected for different purposes and different clients can be Processed separately. This is accomplished by:

- access to data is separated through application security for the appropriate users;
- modules within Service Provider's database separate which data is used for which purpose, i.e. by functionality and function; and

- at the database level, data is stored in different normalized tables, separated per module or function they support; and interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is Processed separately.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. Thus, you are advised to review this page periodically for any changes. We will notify you of any changes by posting the new Privacy Policy on this page. These changes are effective immediately after they are posted on this page.