DATA PROCESSING AGREEMENT (DPA)

This DPA is incorporated by reference into any order form that has as scope SAAS Services and, if the case may be, Advertising Services ("***Order***"/***Order Form***) submitted to by the party identified as "Customer" as set forth in the Order ("***Customer***") and accepted by FastForward.AI Inc. ("***Company***"). By signing the Order Form, Customer acknowledges that it has read and agrees to be legally bound by this DPA. All Order Forms are subject to acceptance by Company.

1. Definitions

Data Protection Laws Means, as applicable, EU General Data Protection Regulation 2016/679 (GDPR) or the mandatory provisions notified to Company in writing of another data protection and privacy law of the applicable jurisdiction in force as relevant to Customer in the receipt and use of the Service and to Company when processing data on behalf of Customer in the provision of the Service;

Controller, Data Subject, Processor, Supervisory Authority, Personal Data, Processing, Data Breach, and other terms shall have the meaning given in the applicable Data Protection Laws.

2. Scope

1. This DPA sets out the rights and obligations of the Customer when acting as data controller and of the Company when acting as data processor, in processing personal data on behalf of the data controller in relation to the Software as a Service Agreement and/or the Advertising Services Agreement, but in all cases without adding to any of the Services or making provision of the Services more onerous for Company.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the Data Protection Laws and this DPA.
2. The data controller has obligation to make adequate decisions about the purposes and means of the processing of personal data.
3. The data controller shall be responsible, among other, for ensuring that all processing of personal data, which the data processor is instructed to perform, has a legal basis.
4. Controller shall be responsible for complying with Data Protection Laws with respect of the performance of its obligations including, and where required

- informs Data subjects about data processing, obtains consent of the Data Subject if required under the law, adequately manages Data Subjects requests;
- ensures all instructions given by it to the Company in respect of Personal Data shall at all times be in accordance with Data Protection Laws
- has the right and legal ground to provide the Personal Data to the Company for the Processing to be performed in relation to the Services

3. The data processor acts according to instructions

1. The data processor shall, within the limits of the Services, process personal data on documented instructions from the data controller specified in this DPA, unless otherwise required to do so by Data Protection Laws to which the processor is subject .
2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the Data Protection Laws, without affecting that controller is the sole responsible for the data processing under the Software as a Service Agreement and/or the Advertising Services Agreement when Company is processor. For clarity, the data controller shall protect and hold harmless the data processor for data processing effected by the latter according to the instructions of the controller.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis.

6. Security of processing

1. Taking into account the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. To this end the data controller evaluated the risks to the rights and freedoms of natural persons inherent in the processing and agrees to the measures mentioned in appendix 1 to this DPA to mitigate those risks to be implemented by the data processor as sufficient.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in this DPA in order to engage another processor (a sub-processor).

2. The data processor has the data controller's general authorization for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

   The list of sub-processors already authorized by the data controller:

   - Software developers and IT&C engineers (like Mobile Professionals)

   - Cloud providers and Cloud operations services (like Amazon)

   - Development, maintenance and support providers (like Secplus Net SRL, Satellite Innovations LLC)
   - Partners that provide access to certain channels (like Infobip in relation to WhatsApp)

3. As at the Effective Date of the Agreement, CUSTOMER understands and agrees that Company's cloud hosting provider, Amazon Web Services EMEA SARL ("Amazon") (a Sub-Processor), has a POP in Dublin, Ireland. If Amazon changes all of its server location outside of the EEA:

- the Company will inform CUSTOMER of the change and the potential financial and service implications of such change on the terms of Agreement, and

- CUSTOMER shall not unreasonably withhold or delay agreement to any consequential variations proposed by the Company to protect itself and its Sub-Processors against additional risks associated with the variations and

- the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the situation as soon as is reasonably practicable

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, similar data protection obligations as set out in the DPA shall be imposed to the extent possible on that sub-processor by way of a contract or other legal act under Data Protection Laws, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the DPA and the Data Protection Laws

8. Transfer of data to third countries or international organizations

1. If restricted under the Data Protection Laws, any transfer of personal data to certain countries or international organizations by the data processor shall only occur in compliance with relevant provisions of Data Protection Laws and is subject to data controller authorization.

9. Assistance to the data controller

1. The Company shall, without adding to the Services or obligations set out in this DPA, directly via the Services and within the limits of the Services as they are at that moment, unless agreed expressly by both parties, promptly provide

such information and assistance (including by taking all appropriate technical and organizational measures), insofar as this is possible, as CUSTOMER may reasonably require in relation to the fulfilment of CUSTOMER's obligations to respond to requests for exercising the Data Subjects' rights under applicable Data Protection Laws taking into account the nature of the processing for the performance of the Services and the information available to the Company.

2. The Company shall, without adding to the Services or obligations set out in this DPA within the limits of the Services unless agreed expressly by both parties, provide such information, co-operation and other assistance to CUSTOMER as CUSTOMER reasonably requires (taking into account the nature of processing and the information available to the Company) to ensure compliance with CUSTOMER's obligations under Data Protection Laws with respect to:

- security of processing according to the technical and organizational measures agreed in this DPA;
- data protection impact assessments (as such term is defined in Data Protection Laws);
- prior consultation with a Data Protection Supervisory Authority regarding high risk processing; and
- any remedial action and/or notifications to be taken in response to any Personal Data Breach and/or any complaint or request relating to either party's obligations under Data Protection Laws relevant to this Agreement, including (subject in each case to CUSTOMER's prior written authorization) regarding any notification of the Personal Data Breach to Data Protection Supervisory Authorities and/or communication to any affected Data Subjects.

11. Erasure and return of data

1. On termination of the provision of personal data processing related to Services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Data Protection Laws requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller the information in its possession that is not protected by confidentiality or non-compete provisions, necessary to demonstrate compliance with the obligations laid down in this DPA and allow audits conducted by the data controller or another auditor mandated by the data controller on the latter expense, based on a written request at least 30 days in advance and maximum once a year. To this end the Company shall provide (or procure) access to relevant premises, systems, personnel and records (subject to the limitations of disclosure of information under applicable competition laws and no access to confidential information like Company's other customers data) during normal business hours for the purposes of each such audit and provide and procure all further reasonable co-operation, access and assistance in relation to any such audit.

2. The data processor shall provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. Commencement and termination

1. The DPA shall apply to personal data processing under the Software as a Service Agreement and/or the Advertising Services Agreement only when Company is acting as processor on behalf of the Customer. The DPA shall apply for the duration of the provision of personal data processing related to the Services within the Term of the Software as a Service Agreement and the Advertising Services Agreement.

14. Changes to DPA

Company may change the DPA at any time and Customer may access the relevant link in the Order Form to the then current version. Using the Services after the changes become effective means Customer agrees to the new terms. If Customer does not agree to the new terms, it must stop using the Services and has the right to terminate the Agreement according to termination clauses.

Appendix 1 to the Data Processing Agreement (DPA)

Data processing and security details

Section 1—Data processing details

Processing of the Personal Data by the Company shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Section 1 of this Appendix 1.

1 Subject-matter of processing:

CUSTOMER is the Data Controller of personal data for the categories of data subjects mentioned herein and uses the Company's Software as a Service and/or Advertising Services. The terms and conditions relating to the use of the Services are governed by the Software as a Service Agreement and the Advertising Services Agreement and this DPA forms an integral part of each of these agreements.

2 Duration of the processing:

The duration of the processing will be for the validity period of the Agreement inside the Term.

3 Nature and purpose of the processing:

CUSTOMER wishes to engage with the categories of data subjects mentioned herein via social media channels through the use of the Company's SaaS Services and/or Advertising Services. The processing of personal data will be undertaken in accordance with the terms of each of the Software as a Service Agreement and the Advertising Services Agreement and this Data Processing DPA.

4 Type of Personal Data:

- Mobile phone number as provided by the User and / or Customer as applicable. Mobile phone number or"MSISDN" means Mobile Station International Subscriber Directory Number as defined by the International Telecommunication Standard Sector recommendation E.164 numbering plan. (by user we mean any mobile user who uses Engagement Channels to access Company Services and to initiate a request or operation that requires fulfilment using the Company Platform)

- Channel ID and Channel user name as used by end-user to log into the relevant Engagement Channel, and as collected from that channel

- User service usage data, profiling preferences and interests based on usage of Company Services alone, or together with other data such as MSISDN:
- User types (to the extent it is personal data)
- Information on end-user account statistics such as account balance inquiries, and any other mobile account-related statistics inquiries
- Personal offers as created by Customer and targeted by Customer systems using MSISDN information and other profiling information from Customer or Company systems as agreed with the Customer
- Other personal data as further instructed by the Customer in writing and agreed with the Customer. By exception from contrary provisions in DPA, Customer may further instruct the Company on other categories of personal data to be processed on its behalf and parties may agree in writing without signing a new document in the form of this Appendix.
- Transactional data including and not restricted to:

o Ordered and or purchased Customer goods or services

o Ordered and or purchased third-party goods or services

o Redeemed vouchers for prepaid Users

o Bill payments to Customer for post-paid Users

o Any other transactions, orders or payments to Customer and any other third-party services

5 Categories of Data Subjects:

Potential customers of CUSTOMER, users of media platforms, visitors on engagements channels, existent clients of CUSTOMER

6 Specific processing instructions:

As per the relevant Order Form, if any.

7 Sub-Processors

Entities mentioned here below shall be deemed as sub processors only to the extent they have access to Protected Data:

- Cloud provider and Cloud operations services (like Amazon Web Services EMEA SARL)
- Software development and customizations, IT&C engineers (like Mobile Professionals LLC)
- Development, maintenance and support (like Secplus Net SRL, Satellite Innovations LLC)
  - Partners that provide access to certain channels (like Infobip in relation to WhatsApp)

8 International Data Transfer

Allowed under the DPA conditions

Section 2—Minimum technical and organisational security measures

1.1 Logical Access Control

To ensure compliance with CUSTOMER's access security control requirements, Company shall commit to:

a) Access or attempt to access only such data for which access has been authorized by CUSTOMER.

b) Protect the confidentiality of all passwords or access codes assigned to Company by CUSTOMER.

c) Protect systems that are hosted for CUSTOMER or which provide critical services on behalf of CUSTOMER such that all access and account credentials are made available to CUSTOMER as needed for troubleshooting, administrative handover, or other purposes that are considered critical to the continuity, availability or integrity of the system or service for CUSTOMER.

d) Company will define a password policy and implement technical controls to enforce the policy. This should include requirements pertaining to the periodic change of passwords and avoidance of trivial or obvious passwords.

e) Timely removal of logical access privileges from Company staff who, whether through internal transfer or departure from Company, become no longer involved in processing CUSTOMER information and data.

f) Company shall implement its own security procedures to ensure that CUSTOMER Data, network connection and Company-owned equipment are secure, and are used only by their authorized employees solely for the intended purposes or as expressly authorized under this Agreement.

g) Customer is the only one responsible for the security of processing through the software and/or hardware owned and/or used by it

1.2 Back-up and Recovery

Company shall commit to:

a) deploying appropriate back-up measures, including the placement of CUSTOMER data files in secure cloud storage and

b) facilitating resumption of critical applications and business activities in a timely manner following an emergency or disaster.

1.3 Company Staff Accountability

To ensure compliance with CUSTOMER's requirements for employee accountability, without affecting other provisions of the Agreement, Company shall commit to using CUSTOMER Data for purposes of the Software as a Service Agreement and the Advertising Services Agreement.

1.4 Security of Databases and Data Files

To ensure the integrity, confidentiality and general security of any and all databases and data files used to store CUSTOMER Personal Data, Company shall commit to:

a) Storing CUSTOMER "Confidential" information (e.g. passwords, customer data, etc.) in a secured format in accordance with COMPANY approved techniques.

b) Restricting physical and logical access to databases, data files and their resident information and/or data and any systems or network components relating to the processing of CUSTOMER Data on a need-to-know / need-to-use business-only basis.

c) Protecting all access to databases and data files that contain CUSTOMER data using, at a minimum in accordance with industry norm for password.

d) Changing all factory pre-set passwords for databases before commencement of processing and changing them periodically.

e) Logging database and data file access activities and storing this activity data to the extent permitted by the Services and related systems

f) Logging CUSTOMER Data transaction activities and storing this activity data to the extent permitted by the Services and related systems

g) Handling all back-up copies of all database if any and data file records according to safe-keeping measures and access controls, with such controls identical or similar to those employed for the primary database or data files.

h) Deploying database security tools to periodically review database configurations and ensure compliance with expected base configurations.

i) Deleting and destroying, when there is the case, in a secure manner all instances of any and all CUSTOMER information and/or data to ensure that transaction and other data cannot be recovered by unauthorized persons.

j) Reviewing all database security controls defined above on a periodic basis (at least once per year) to ensure that they are still in effect.

1.5 Other minimum requirements

Company shall commit to minimum internal best practices while handling Personal data:

a) Company computers must never be left unattended while in use and must have screen locking mechanisms to prevent unauthorized access to data with the requirement to re-enter their login credentials to resume working on their computers.

b) Documents that are created by individuals, which contain Personal Data, should not be kept on computer desktop folders that can be easily accessed by others, unless it is password protected or encrypted.