HAPPYML, LLC

Security Agreement

Objectives

1. HappyML and Customer have entered into, and may in the future enter into, one or more agreements (each a "Services Agreement") whereby HappyML will provide Customer with access to HappyML's Services. HappyML shall implement data security measures that are consistent with industry best practices and standards so that HappyML:

a) Protects the privacy, confidentiality, integrity, and availability of all data which is disclosed by Customer to or otherwise comes into the possession of HappyML ("Customer Data"), its affiliates or sub-contractors, directly or indirectly as a result of a Services Agreement, including but not limited to Customer's Confidential Information and any Customer personally identifiable information;
b) Protects against accidental, unauthorized, unauthenticated, or unlawful access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of the Customer Data including, but not limited to, identity theft;
c) Complies with all federal, state, and local laws, rules, regulations, directives and decisions (each, to the extent having the force of law) that are relevant to the handling, processing, storing or use of Customer Data by HappyML in accordance with this Agreement;
d) Manages, controls and remediates any threats that HappyML identifies in its internal review of its security practices that could result in unauthorized access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of any of the Customer Data, including without limitation identity theft; and
e) Complies with and implements the risk policies listed in this document, together with the data protection and confidentiality obligations of the Services Agreement.

Organization Security Measures:

1. Certification: HappyML shall comply with the Payment Card Industry (PCI) Data Security Standard (DSS) throughout the provision of Services to Customer. Upon Customer's request, one time per calendar year, HappyML will provide Customer with an unexpired PCI DSS Attestation of Compliance (for Level 2 compliance) against the then-current version of the DSS.

2. Environment: HappyML shall provide assurance that it sets the foundation for the necessary tone, discipline, and structure to influence the control consciousness of its people necessary, and for the services provided to Customer.

3. Responsibility: HappyML shall assign responsibility for information security management to appropriate skilled and senior personnel.

4. Qualification of Employees: HappyML shall implement and maintain appropriate security measures and procedures, including background checks following industry best practices, to restrict access to information systems used in connection with the Services Agreement or to Customer Data to only those personnel who are reliable, have sufficient technical expertise for the role assigned, and have personal integrity.

5. Obligations of Employees: HappyML shall implement and maintain appropriate security measures and procedures in order to verify that any personnel accessing the Customer Data or information systems used in connection with the Services Agreement knows his or her obligations and the consequences of any security breach.

6. Segregation of Duties: HappyML shall provide reasonable assurance the organization of personnel provides adequate segregation of duties between incompatible functions.

Physical Security Measures:

1. Physical Security and Access Control: HappyML shall ensure that all systems hosting Customer Data and/or providing services on behalf of Customer are maintained consistent with industry best practices and standards in a physically secure environment that prevents unauthorized access, with access restrictions at physical locations containing Customer Data designed and implemented to permit access only to authorized individuals and to detect any unauthorized access that may occur.

2. Physical Security for Media: HappyML shall implement and maintain appropriate security measures and procedures consistent with industry best practices and standards to prevent the unauthorized viewing, copying, alteration or removal of any media containing Customer Data, wherever located.

3. Media Destruction: HappyML shall implement and maintain appropriate security measures and procedures consistent with industry best practices and standards to destroy removable media and any mobile device (such as discs, USS drives, DVDs, back-up tapes, laptops and phones) containing Customer Data where that media or mobile device is no longer used, or alternatively to render Customer Data on that removable media or mobile device unintelligible and not capable of reconstruction by any technical means before re- use of the removable media is allowed.

Computer System Access Control Measures:

1. Access Controls: HappyML shall implement and maintain appropriate security measures and procedures consistent with industry best practices and standards to ensure the logical separation so that access to all systems hosting Customer Data and/or being used to provide services to Customer shall: be protected through the use of access control systems that uniquely identify each individual requiring access, grant access only to authorized individuals and based on the principle of least privileges, prevent unauthorized persons from gaining access to Customer Data, appropriately limit and control the scope of

access granted to any authorized person, and log all relevant access events. These security measures and procedures shall include, but shall not be limited to:

a. Access Rights Policies: HappyML shall implement appropriate policies and procedures regarding the granting of access rights to Customer Data in HappyML's possession or control, in order to ensure that only the personnel expressly authorized pursuant to the terms of the Services Agreement or by Customer in writing may create, modify or cancel the rights of access of the personnel. HappyML shall maintain an accurate and up to date list of all personnel who have access to the Customer Data and shall have the facility to promptly disable access by any individual personnel. For purposes of this Schedule, the term "personnel" as to Customer or HappyML shall mean a Party's employees, consultants, subcontractor or other agents.

Intrusion Detection/Prevention and Malware

HappyML shall use appropriate security measures and procedures

(a) to ensure that Customer Data in HappyML's possession and control, and /or systems being used to provide Services, is protected against the risk of intrusion and the effects of viruses, Trojan horses, worms, and other forms of malware, and

(b) to monitor and record each and every instance of access to the HappyML's assets and information systems and to Customer Data to detect the same, and to promptly respond to the same.

If any malicious code is found to have been introduced by HappyML or any third party into any of HappyML's information systems handling or holding Customer Data, HappyML shall take appropriate measures to prevent any unauthorized access or disclosure of any Customer Data and in any case (wherever the code originated), HappyML shall, at no additional charge to Customer, remove the malicious code and eliminate the effects of the malicious code. If the malicious code causes a loss of operational efficiency or loss of data, HappyML shall monitor the losses and restore lost data in accordance with the terms of the Agreement. Unless, and to the extent, prohibited by law enforcement authorities, HappyML shall immediately notify Customer's Chief Information Security Officer if it knows or reasonably suspects that there has been an actual instances of unauthorized access to the Customer Data and/or systems holding or handling Customer Data and shall cooperate fully in assisting Customer as necessary to enable Customer to comply with its statutory and other legal breach notice requirements, if any.

HappyML Obligations

1. Implement and maintain appropriate incident response measures and procedures for systems that handle or hold Customer Data

2. Ensure that all networks holding Customer Data are routinely monitored so that operational problems and security incidents are detected, reported, logged, and resolved in a timely manner.

3. In the unlikely event that applicable law requires HappyML to process Customer Data other than pursuant to Customer's instructions, HappyML will notify Customer (unless prohibited from so doing by applicable law);

4. Without undue delay upon becoming aware, inform Customer if, in HappyML's opinion, any instructions provided by Customer infringe 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 that data ("GDPR");

5. As soon as reasonably practicable upon becoming aware, notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data in HappyML's possession or under its control (including when transmitted, stored or otherwise processed by HappyML) (a "Security Breach");

6. Taking into account the nature of the processing, promptly provide Customer with reasonable cooperation and assistance in respect of the Security Breach and all information in HappyML's possession concerning the Security Breach, including, to the extent known to HappyML, the following:

- the possible cause and consequences of the Security Breach;
- the categories of Customer Data involved;
- a summary of the possible consequences for the relevant data subjects;
- a summary of the unauthorized recipients of the Customer Data; and
- the measures taken by HappyML to mitigate any damage;

7. Unless required to make a disclosure or announcement by applicable law, insofar as a Security Breach relates to Customer, not make any announcement about a Security Breach (a "Breach Notice") without:

- the prior written consent from Customer; and
- prior written approval by Customer of the content, media and timing of the Breach Notice;

8. Taking into account the nature of processing and the information available to HappyML, assist Customer when reasonably requested in relation to Customer's obligations under EU Data Protection Laws with respect to:

- data protection impact assessments (as that term is defined in the GDPR);
- notifications to the supervisory authority under EU Data Protection Laws and/or communications to data subjects by Customer in response to any Security Breach; and
- Customer's compliance with its obligations under the GDPR with respect to the security of processing.

9. Taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, to respond to data subjects' requests to exercise their rights under Chapter III of the GDPR. HappyML will promptly notify Customer of requests received by HappyML, unless otherwise required by applicable law. Customer may make changes to Customer Data processed with the Services. Except as required by law, HappyML will not make changes to that data except as agreed in writing with Customer.

10. Maintain records of its processing activities as required by Article 30.2 of the GDPR, and make those records available to the applicable supervisory authority upon request.

Data Management Controls Measures

1. Customer Data: Customer Data must only be used by HappyML for the purposes specified in the Services Agreement.

2. Data Integrity Controls: HappyML will implement and maintain appropriate security measures and procedures to protect the integrity of the Customer Data in HappyML's possession or control, to prevent the unauthorized recording, alteration or erasure of Customer Data, and to ensure that it is subsequently possible to determine when, by whom and which Customer Data were recorded, altered or erased.

3. Data Destruction: HappyML will implement and maintain appropriate security measures and procedures to destroy Customer Data in HappyML's possession or control when appropriate and in accordance with the Services Agreement. At the request of Customer at any time, HappyML will: (i) promptly return to Customer, in the format and on the media reasonably requested by Customer, all or any part of Customer Data; and (ii) erase or destroy all or any part of Customer Data in HappyML's possession, in each case to the extent so requested by Customer. Customer acknowledges that HappyML will have no liability for any limit on its ability to provide the Services as a result of HappyML's compliance with Customer's request during any Services Term.

4. Software Patching: HappyML will implement and maintain appropriate security measures and procedures in order to ensure the regular update and patching of all computer software on systems that handle or hold Customer Data to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches.