APPENDIX 2
Summary of security measures implemented by Indiegogo

This document describes security measures that Indiegogo has implemented to ensure that Creator Data is processed in accordance with the Applicable Data Protection Laws and the DPA. This document is regularly updated to reflect changes made in Indiegogo's security and data privacy compliance program.

1. General organizational measures

a. **Data Protection Officer**. Indiegogo has appointed a Data Protection Officer who is responsible for coordinating, monitoring and improving Indiegogo's security. The Data Protection Officer is responsible for coordinating, monitoring and improving data protection related issues.
b. **Confidentiality**. Indiegogo's entire personnel is subject to confidentiality obligations and may only access personal data (personal information) subject to a prior, written authorization issued by Indiegogo.
c. **Compliance Program**. Indiegogo has introduced a Compliance Program to help ensure that all campaigns on the platform adhere to relevant legal and regulatory standards, including data protection, advertising, and consumer rights.

2. Training and awareness

a. **Personnel training**. Indiegogo conducts regular training sessions for its personnel on data protection rules and personnel roles within its Compliance Program. Indiegogo also informs its personnel about possible consequences of non-compliance. These training sessions are conducted using anonymized data.

3. Physical and environmental security

a. **Access to data**. Indiegogo implements comprehensive security measures, including encrypted access to personal data, secure storage, periodic password updates, and strict access controls to ensure the confidentiality and integrity of user data.
b. **Protection from disruptions**. Indiegogo takes reasonable measures per industry accepted solutions to protect against loss of data due to power supply failure, fire, natural disaster or line interference.
c. **Component disposal**. Indiegogo takes reasonable measures per industry accepted solutions to delete Creator Data when it is no longer needed.

4. Access control

a. **Access authorization**. Access to personal data is restricted to authorized personnel only, with the use of encrypted channels (e.g., VPN, secure email) for external access. Physical data is stored in secured rooms and cabinets, while data access within the LAN is limited to designated servers Additionally, Indiegogo adheres to industry-standard protocols for the timely deactivation of passwords that have been compromised or inadvertently disclosed.
b. **Limitation of privileges**. A restricted and designated group of personnel is exclusively authorized to grant, modify, or revoke access privileges to Indiegogo's facilities and information systems. User accounts are configured with the minimum privileges necessary to perform their tasks. Workstations are protected by accounts without administrative rights, and laptops are encrypted to prevent unauthorized access.
c. **Authentication of users**. Indiegogo employs industry-recognized solutions, including multifactor authentication, to identify and authenticate users accessing its information technology systems. Passwords are regularly updated and must conform to minimum standards established by Indiegogo's security policies. Additionally, best practices are rigorously applied to ensure the confidentiality and integrity of passwords during assignment, distribution, and storage. These measures are designed to safeguard credentials and prevent unauthorized access to Indiegogo's IT systems, in line with recognized security protocols.
d. **Monitoring**. Indiegogo continuously monitors its information systems to detect and prevent any attempts of unauthorized access, including the use of expired or invalid credentials. All access to

servers is logged and monitored, including both successful and unsuccessful attempts. Indiegogo maintains comprehensive documentation of security measures and records any data protection incidents, ensuring accountability and traceability.

5. Asset and operations management

a. **Endpoint protection**. All computing endpoints are encrypted and protected against malware.
b. **Backup copies**. Indiegogo regularly creates backups of service settings, configuration details, and Creator Users' Data. These backups are maintained to ensure data integrity, continuity of operations, and the ability to restore critical information in the event of system disruptions or data loss, in accordance with Indiegogo's data protection and security protocols.
c. **Integrity and confidentiality**. All team members are required to log out of all active sessions when stepping away from their workstations, regardless of location, to prevent unauthorized access. Indiegogo maintains the integrity and confidentiality of personal data through access controls, secure storage (physically and digitally), and encryption. The system is designed to prevent unauthorized access, ensure the authenticity of the data, and protect it from tampering or breaches.

6. Incident management

a. **Malicious software**. Indiegogo has implemented comprehensive anti-malware controls to prevent malicious software from gaining unauthorized access to Creator Data and its information systems. These controls are designed to safeguard against threats originating from public networks, ensuring the protection of data and the integrity of Indiegogo's systems in compliance with established security standards and best practices.
b. **Incident record**. Indiegogo maintains a detailed record of all security incidents, which includes the date and time of each incident, the consequences resulting from the breach, and the corrective measures implemented to prevent recurrence. This documentation ensures a systematic approach to incident management and enhances the organization's ability to mitigate future security risks in alignment with industry best practices and legal obligations.
c. **Service monitoring**. Indiegogo conducts regular verification and monitoring of system logs to detect any irregularities or suspicious activity. This continuous oversight is implemented to promptly identify potential security threats and ensure the integrity and security of Indiegogo's information systems, in accordance with its established security policies and procedures.