ACTIVITIES LOG OF DATA PROCESSOR (GENERAL)

1. Identification of the Processing organisation

In accordance with the provisions of Regulation (EU) 2016/679 of 27 April 2016 (GDPR), the Processing organisation is who will carry out processing activities on behalf of a Controller.

Tax number	STOCKCROWD FANRAISING, S.L.
TIN	B67084558
Activity	FINANTIAL SERVICES
Address	c/ Bruc, 145 - Entlo. 2 08037 BARCELONA (Barcelona)
Telephone	93 676 14 17
E-mail	info@stockcrowd.com
Trademark	STOCKCROWD FANRAISING, S.L.
Web	stockcrowd.com
Email AEPD Notification	infodat@stockcrowd.com
Email exercise rights	infodat@stockcrowd.com
Legal representative	Sergio Pallares Nadal, Javier Villacampa Ecequiel
Security Officer (DSPO)	Sergio Pallares Nadal

2. Identification of personal data files processed on someone else's behalf

A filing system is a structured set of personal data accessible in accordance with certain pre-set criteria and liable to processing for specific purposes.

Filing system	Description	Type	System	Category
5 CROWDFUNDING CAMPAINGS MANAGEMENT	Platform support, configuration and maintenance. Management of the fans and donors of the campaigns created by the promoters.	Processor	Mixed	BASIC

3. Register of processing activities

In accordance with the provisions of Article 30 of Regulation (EU) 2016/679 of 27 April 2016 (GDPR), the Processor must keep and update a Register of processing activities completed under their responsibility, electronically, which contains:

- Name and contact details of each Data Controller on whose behalf the Officer is acting and, where applicable, of the Controller's Representative and of the Data Protection Officer (DPO).

- Purposes of the processing.
- Description of the categories of Data Subject.
- Breakdown of the categories of data.
- Data transfers to third party countries, with identification of these with documentation of appropriate guarantees.
- Whenever possible:
    - General description of technical and organisational security measures.

The Controller, or their Representatives, must make this Register of activities available to the Spanish Supervisory Authorities upon request.

This Register documents each of the Files described in section 2 and are detailed below. The technical and organisational measures implemented by the Organisation by design and by default, in all phases of the processing are detailed at the end of the document.

5. CROWDFUNDING CAMPAINGS MANAGEMENT

Description	Platform support, configuration and maintenance. Management of the fans and donors of the campaigns created by the promoters.
Processing system	Partially automated
Data source	The data subject or a legal representative
Purposes	Other purposes: Provision of electronic communication services, Advertising and commercial research
Categories of data subjects	Clients and users
Categories of data	
Identification data	National ID (DNI) or tax ID (NIF) number, Name and surnames, Postal or email address, Telephone
Special or criminal data categories	Do not exist
Other type of data	Personal characteristics, Economic, financial and insurance, Transactions of goods and services
Categories of recipients	
Transfers	Organizations or people directly related to the controller. Other finantial entities.
International transfers	Do not exist
Timelines for data erasure	Stored IN ACCORDANCE WITH the instructions of the Controller
Security measures	
General description of technical and organisational security measures	The technical and organisational security measures implemented are aimed at ensuring, in particular: control of physical access to the equipment where the data are processed, control of the media that may contain the personal data, control of the storage of the data, control of the users authorised to access the data and the type of access they have, control of the transmission of the data and their transport, and control of the availability and integrity of the data.

Order controllers

..... ()	.....	.....	
THYSSEN ()	--	-	(Madrid)

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Premises or Offices

SEDE FISCAL	Measures	Risk
Type of access to the premises	Unrestricted entry with access control (reception staff, security guards, etc.).	Low risk
General key control system	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures	THERE ARE NO security measures.	Low risk

Departments

DEPARTAMENTO TÉCNICO	Measures	Risk
Permit:	Limited to authorised staff in the workstations and document archives.	Low risk
Access:	Access to the Department governed by the security measures of the Premises.	Low risk
Password control:	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures:	THERE ARE NO other security measures.	Low risk

PROYECTOS	Measures	Risk
Permit:	Limited to authorised staff in the workstations and document archives.	Low risk
Access:	Access to the Department governed by the security measures of the Premises.	Low risk
Password control:	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures:	THERE ARE NO other security measures.	Low risk

DESARROLLO DE NEGOCIO	Measures	Risk
Permit:	Limited to authorised staff in the whole Department.	Low risk
Access:	Access to the Department governed by the security measures of the Premises.	Low risk

Password control:	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures:	THERE ARE NO other security measures.	Low risk

SOPORTE A CLIENTES	Measures	Risk
Permit:	Limited to authorised staff in the workstations and document archives.	Low risk
Access:	Access to the Department governed by the security measures of the Premises.	Low risk
Password control:	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures:	THERE ARE NO other security measures.	Low risk

MARKETING	Measures	Risk
Permit:	Limited to authorised staff in the workstations and document archives.	Low risk
Access:	Access to the Department governed by the security measures of the Premises.	Low risk
Password control:	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures:	THERE ARE NO other security measures.	Low risk

COMERCIAL	Measures	Risk
Permit:	Limited to authorised staff in the workstations and document archives.	Low risk
Access:	Access to the Department governed by the security measures of the Premises.	Low risk
Password control:	The keys are stored in a secure place which requires authorised access.	Low risk
Other security measures:	THERE ARE NO other security measures.	Low risk

Confidentiality of information

Information on the processing for the data subject	Measures	Risk
Is the Data Subject informed of the details of the processing?	Yes, with personalised data protection clauses.	Low risk
Has the Data Subject been informed of their rights?	Yes, with personalised data protection clauses.	Low risk
Transport and transfer of data	Measures	Risk
Transfer of storage media within the company	By staff authorised by the Data Controller with security measures.	Low risk
Transfer of storage media beyond the company	By staff authorised by the Data Controller with security measures.	Low risk
Automated data procedures (digital)	Measures	Risk
Access during digital processing (screens)	The data is processed by preventing unauthorised persons from viewing the data.	Low risk
Storage of the digital storage media	It is stored in a Cabinet and/or Department with security measures.	Low risk
Destruction of the digital storage media	Digital storage media destroyer.	Low risk
Non-automated data procedures (documents)	Measures	Risk
Access during manual processing (documents)	It is processed preventing unauthorised persons from accessing the data.	Low risk
Document storage	It is stored in a Cabinet and/or Department with security measures.	Low risk
Document shredding	Paper shredder.	Low risk
Register of access to special categories of data	Measures	Risk
Is a record taken of logins to special data categories?	Special categories of data ARE NOT PROCESSED.	No risk

09 Network

Access to IT equipment	Measures	Risk
Control of access to IT devices	Personalised username and password.	Low risk
Control of access to personal data records	Access to the records and/or program through a password.	Low risk
Access to IT networks	Measures	Risk
Direct access to information systems (network connection)	Personalised username and password.	Low risk
Wireless access to IT systems (Wi-Fi, Bluetooth, etc.)	Restricted access by security code.	Low risk
Remote access to information systems	Personalised username and password.	Low risk
Encryption of remote connections	Yes.	Low risk

Identification and authentication system	Measures	Risk
Identification system (USERNAME)	Personalised password for each user.	Low risk
Authentication system (PASSWORD)	Personalised password for each user.	Low risk
Encryption of the password	The password is encrypted	Low risk
Combination of characters	The password consists of at least 8 characters, with at least one number, one upper case letter, one lower case letter and a symbol or a special character	Low risk
Repeated attempts to login	The system has been implemented to prevent repeated unauthorised attempts	Low risk
Expiry of the password	The password is changed at least once a year	Low risk

Information integrity

Backup copies	Measures	Risk
Location of the copies	It is stored in Hardware other than that which created it (network copy).	Low risk
Frequency of scheduling	At least weekly.	Low risk
Data verification frequency	At most 6 months after creation.	Low risk
Data verification method	Copy verification software.	Low risk
External backup copies	Measures	Risk
Location of external copies	Premises or department other than where it was created.	Low risk
Frequency of scheduling external copies	At least weekly.	Low risk
Encryption of the data of the external copies	Copies are not encrypted because they do not leave the company's premises.	No risk
Availability of the data	Measures	Risk
Availability of the information services	THERE ARE measures to guarantee the availability of the data	Low risk
Restoration of the information services	THERE ARE measures to rapidly restore availability and access to the data	Low risk
Resilience of the information services	THERE ARE measures to anticipate and adapt to unforeseen changes in the information services	Low risk
Security measure verification and assessment processes	PROCESSES HAVE BEEN ESTABLISHED to verify or assess the effectiveness of the security measures	Low risk

Specific treatments

Specific processing	Measures	Risk
Processing of data of children younger than 14 years old	The data of children younger than 14 years old IS NOT PROCESSED	No risk
Infringement of fundamental rights and freedoms	NO processing infringing fundamental rights or freedoms IS PERFORMED	No risk

Internet

Electronic communications	Measures	Risk
Secure email	Secure email using point-to-point encryption IS USED.	Low risk
Data protection clause	A data protection clause with adequate data processing information HAS BEEN PUBLISHED.	Low risk

Organización

Organisation	Measures	Risk
Information Policy	THERE IS a documented protocol for informing and communicating the processing to the data subject	Low risk
Rights of the Data Subject	THERE IS a documented protocol for managing and recording the rights of the data subject	Low risk
Security Policy	THERE IS a documented protocol guaranteeing the security of the personal data and its protection from DESIGN AND DEFAULT	Low risk
Security breaches	THERE IS a documented protocol for managing and recording security breaches	Low risk
Data protection training	[Adequate training is provided to staff authorised to process data] through the publication of the security policy	Low risk
Data Protection Officer (DPO)	[A DPO is not required because the company's core business] CONSISTS in processing personal data but NOT on a LARGE SCALE, nor regulated in art. 34 of the LOPDGDD.	Low risk
Impact assessment (DPIA)	[It is not necessary to carry out a DPIA because] the processing is not likely to result in a high risk for the rights and freedoms of natural persons.	Low risk