SECURITY PROTOCOL - PERSONAL DATA PROCESSING

NEED TO ANALYZE RISKS

Regulation (EU) 2016/679, of General Data Protection (RGPD) requires the adoption of **appropriate technical and organizational measures** in order to guarantee the protection of the rights and freedoms of natural persons regarding the processing of personal data.

In order to be able to demonstrate compliance with the GDPR, the data controller must adopt internal policies and apply security measures that comply with the principles of data protection by design and by default.

In addition, **inherent risks to the processing must be assessed and measures applied to mitigate them**. These measures must guarantee an appropriate level of security, including confidentiality, taking into account the state of the art and the cost of its application regarding the risks and the nature of the personal data to be protected.

When peforming risk assessment related to data security, the risks arising from the processing of personal data must be taken into account, such as the destruction, loss or accidental or illegal alteration of personal data transmitted, stored or processed by another way, or the unauthorized communication or access to these data, susceptible in particular to cause physical, material or immaterial damages.

Thus, this document contains the principles that STOCKCROWD FANRAISING, S.L. must apply to the data processing carried out, from their collection (either from the interested party or from a third party), until their removal, when they are no longer necessary for the purposes for which they were collected.

In the same way, this document contains the **minimum technical and organizational measures** that STOCKCROWD FANRAISING, S.L. must apply to the data processing, according to the previous risk analysis, and which are necessary to guarantee the security of the personal data processed.

SECURITY MEASURES APPLIED TO AUTOMATED PROCESSING

Staff tasks and obligations

The tasks and obligations of each of the users or user profiles with access to personal data and to the information systems will be clearly defined and documented.

STOCKCROWD FANRAISING, S.L. will adopt the necessary measures so that the staff knows in an understandable way the security regulations that affect the development of their functions as well as the consequences that could be incurred in case of non-compliance.

- **Access control**

Users must have access only to those resources they need for the development of their functions. STOCKCROWD FANRAISING, S.L. will ensure that there is an up-to-date list of users and user profiles, and the authorized accesses for each of them. This can be achieved by keeping the information updated on the MICROLAB platform, in relation to staff profiles.

STOCKCROWD FANRAISING, S.L. will also establish mechanisms to prevent a user from accessing different resources from those authorized. Only the personnel authorized to do so may grant, alter or cancel the authorized access to the resources.
In the event that there are personnel outside the STOCKCROWD FANRAISING, S.L. organization who have access to the resources, they must be subject to the same security conditions and obligations as the own personnel.

- **Media and document management**

Media and documents that contain personal data must allow the identification of the type of information they contain, be inventoried and must only be accessible by the personnel authorized to do so, although these obligations are excepted when the physical characteristics of the data carrier make it impossible to fulfill them.
The output of data carriers and documents containing personal data outside the premises under the control of STOCKCROWD FANRAISING, S.L., must be authorized by it. In the transfer of documentation, measures will be taken to avoid theft, loss or unauthorised access to the information during its transport.

Moreover, whenever any document or medium containing personal data is going to be discarded, it must be destroyed or erased, through the adoption of measures aimed at preventing access to the information contained therein or its subsequent recovery.

The identification of the data carriers containing personal data which are considered especially sensitive by the organization may be carried out using understandable and meaningful labeling systems, for example by the use of codes, that allow users with authorized access to identify their content, and that hinder the identification to other people.

- **Identification and authentication (PASSWORDS)**

STOCKCROWD FANRAISING, S.L. shall adopt the measures that guarantee the correct identification and authentication of the users, establishing a mechanism that allows the unequivocal and personalized identification of any user who tries to access the information system as well as the verification that they are authorized.
When the authentication mechanism is based on the existence of passwords, there will be an allocation, distribution and storage procedure that guarantees their confidentiality and integrity. The password change interval in no case will exceed one year and, while they are in force, they will be stored in an unintelligible way.
To access the computer systems, a username and password must be required.

Types of passwords that contain people's names, or user names, date of birth, ID, etc. should be avoided. It is recommended to set up the System Directives in Windows to specify the level of complexity of the passwords.

For a password to be safe, it must contain at least eight characters made up of letters, numbers, and symbols.

- **Backup copies and recovery**

Action procedures must be established for making backup copies at least weekly, unless there has been no update of the data in that period.

In the same way, procedures will be established for the recovery of the data that guarantee at all times its reconstruction in the state in which they were when the loss or destruction took place.

STOCKCROWD FANRAISING, S.L. will be in charge of verifying every six months the correct definition, operation and application of the procedures for making backup copies and data recovery.

In addition, a backup copy of the data and the recovery procedures must be kept in a different place from the one where the computer system that processes them is located, which must comply in any case with the security measures required in this document, or using elements that guarantee the integrity and recovery of the information, so that its recovery is possible.

The tests prior to the implementation or modification of the information systems that process files with personal data will not be carried out with real data, unless the level of security corresponding to the processing carried out is ensured. If you plan to carry out tests with real data, you must have previously made a backup copy.

- **Screen lock**

The screen lock should be activated when there is no activity. In the Windows / Control Panel settings, the screen lock with time interval must be activated to safeguard possible personal data information and prevent it from being viewed by unauthorized persons.
Disabling the screen lock must require a password.

- **Protection control against external threats**

You must have a properly updated antivirus in order to avoid as far as possible new variants of viruses and threats that appear every day.

In addition, periodic reviews of security systems should be carried out. It is convenient to check that all the parameters are working correctly, check the security logs, antivirus, firewall, etc.

- **Control of installed software**

All administration software licenses installed on computers must be original it is necessary to have an inventory.

Original licenses must be installed to keep the operating systems updated in order to benefit from the new versions that in many cases incorporate utilities and security patches and, where appropriate, to be able to activate the security updates included in Windows.

In addition, it is highly recommended to perform security updates (in the case of Windows, through Windows Update), to download the latest security updates fully automatically.

- **Security measures to be applied in tablets and smartphones**

Due to the ease of use of these devices, they have become popular both in professional and domestic areas, being used for all types of processing operations. For this reason, the security measures to be applied in these devices must be as strict as those applied in the organization’s computer system:

- Installation of security applications: there is a wide variety of these types of applications on the market, designed to protect the device from viruses and other attacks. In addition, many of them allow remote blocking and erasure in case of theft or loss.

- Firm lock: the device must be protected with a pattern or password (the second option is safer) that is unique and strong. It is also necessary to change it with the same periodicity as the password of the computer equipment.

- Use of applications: the installation of applications that are unnecessary for professional work should be avoided. In addition, only official and legitimate applications should be installed, using only secure stores, such as Google Play and App Store.

- Avoid public WiFi: connection to public WiFi networks should be avoided by all means, as these types of networks seriously compromise the integrity of the information contained in the device, and may be accessible to third parties with computer knowledge.

- **Security breaches**

The GDPR defines a personal data breach as "any breach of security leading to the accidental or unlawful destruction, loss,

alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

will document any personal data breach, including the facts related to it, its effects and the corrective measures taken.

.As soon as STOCKCROWD FANRAISING, S.L. becomes aware of a personal data breach, it shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Spanish Data Protection Agency, unless it can demonstrate the improbability that the violation of the security of personal data entails a RISK for the rights and freedoms of natural persons. That is, the security violation must be notified to the Spanish Data Protection Agency when it constitutes a RISK for the rights and freedoms of the interested parties.
This notificación shall at least:

1. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained
3. Describe the likely consequences of the personal data breach;
4. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, STOCKCROWD FANRAISING, S.L.shall communicate the personal data breach to the data subject without undue delay.
The communication to the data subject shall describe in clear and plain language the nature of the personal data breach, the name and contact details of the data protection officer or other contact point, describe the likely consequences of the personal data breach as well as the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

However, the communication to the data subject referred shall not be required if:
a. STOCKCROWD FANRAISING, S.L. has implemented appropriate technical and organisational protection measures, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b. STOCKCROWD FANRAISING, S.L. has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
STOCKCROWD FANRAISING, S.L. must implement a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the processing.

Extraordinarily, such verification must be carried out whenever substantial modifications are made to the information system that may affect compliance with the security measures implemented in order to verify their adaptation, adequacy and effectiveness.

SECURITY MEASURES APPLIED TO NOT AUTOMATED PROCESSING (PAPER)

In addition to applying the measures described above which can be logically transferred to the processing of data on non-automated media or on paper, the following measures must be applied, in order to guarantee the security of this type of processing.

- **Flie criteria**

The file of carriers or documents will be carried out in accordance with the criteria provided in their respective legislation. These criteria must guarantee the correct storage of the documents, the location and consultation of the information and enable the exercise of the rights of opposition to the processing, access, rectification and erasure.

In those cases in which there is no applicable rule, STOCKCROWD FANRAISING, S.L. must establish the criteria and action procedures that must be followed for the file.

- **Storage devices**

Storage devices for documents containing personal data must have mechanisms that hinder their opening. When their physical characteristics do not allow the adoption of this measure, STOCKCROWD FANRAISING, S.L. will adopt measures that prevent access by unauthorized persons.

- **Safeguard of carriers**

As long as the documentation with personal data is not archived in the storage devices, because it is in the process of review or processing, either before or after its filing, the person in charge must safeguard it and prevent at any time that it can be accessed by unauthorized persons.

- **Information destruction**

When it is necessary to dispose of the documentation containing personal data, it must be destroyed in such a way as to prevent the possible recovery of the information. For this, it is highly recommended to use a paper shredder.