SECURITY POLICY

www.artizan.ma

March 2019

Table of contents

PURPOSE, SCOPE AND USERS

SINERGIA VENTURES LTD, hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Company operates. This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to the Company and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

This Security Policy details how and to what extent Sinergia assures the security, meaning the control and the access, of the data it collects, stores, process, and more generally of all Sinergia’s information resources. In regard of the the EU General Data Protection Regulation (EU 2016/679), this document aims to ensure Sinergia covers all data security requirements.

This Policy applies to the Company and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of The Company.

Reference Documents

EU GDPR 2016/679 (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 such data, and repealing Directive 95/46/EC).

1. ROLES AND RESPONSIBILITIES

1.1. Within Sinergia

Our Chief Information Security officer acts as Sinergia's Security Officer. He can be contacted at RSSI@artizan.ma. His responsibilities includes:

- the control and maintenance of all Sinergia's information resources
- management of the development team to supervise all changes made to the source code
- management of the sysadmin team to supervise all infrastructure decision

Following the EU General Data Protection Regulation, Sinergia has nominated a Data Protection Officer (DPO) who can be contacted on GDPR@artizan.ma. His responsibilities includes :

- Educating the company and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR Supervisory Authorities
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request

1.2. Outsourcing

Contabo GmbH. is our hosting provider. It's role is to handle our hosting and web servers. They setup the machines and supervise the hardware in their own datacenters in Germany. It's role is to provide a space to host our servers. They control physical access to our machines.

2. ACCESS & STORAGE

2.1. Business facilities

Access to business location is controlled by a badge/key system. Facilities surveillance is monitored by cameras.

2.2. Storage

- Data is stored in Germany/Europe only. It can be accessed from anywhere in the world as long as an authorized login/password is used.

- Country restrictions can be applied on a per account basis to limit the countries from where a login can be authorized.
- Sinergia relies on system level protections : server login is restricted to administrators using SSH keys (no passwords).
- Data at rest is not encrypted.

2.3. Storage Period Limitation

Personal data must be kept and is kept for no longer than is necessary for the purposes for which the personal data are processed.

2.4. Applications

- Our application ensures that data given by our partner can only be seen by our partner or our employees (in order to follow up on our contractual engagement).
- We have a login/password authentication to our interface, for Sinergia coworkers, clients and suppliers.
- Password complexity rule is a 8 characters minimum. Passwords are hashed using several rounds of sha256 and a random salt

2.5. Logs and access to logs

- The amount of logged information is too large to be detailed. Sinergia logs all type of information and actions on the interface, on the web server…
- Logs are stored in databases and/or files. Their duration of storage depends of the type of log (access logs, actions logs…), it could vary from infinite to a couple of days.
- Sinergia business partners can access to logs on request to its CTO. Request will be accepted or not depending on its legitimacy.

2.6. Device security

All Sinergia employees use device protected by Kaspersky antivirus and automatic updates.

3. AUDIT

Sinergia's business partners are welcome to audit Sinergia procedures with the necessary limitation to ensure privacy of our clients and suppliers. A technical audit of the Sinergia platform is done every year by CISO and Certified Ethical Hackers.

4. DATA

4.1. Personal data

- All personal data and categories of data collected, stored and processed by Sinergia on behalf of its client are kept in a record of operations available anytime given upon request after validation of our CTO. This record of operation details all purpose and legal basis of each processing activity.
- Sinergia do not use any personal data for any other purpose that the ones described it the record of processing.
- When possible, Sinergia stores a pseudonym of the personal data via MD5 hash.

4.2. Data accessibility

- Most of personal data Sinergia processes isn't accessible by it's empoyees, yet some of it can be. In that case it can be accessible from anywhere in the world by connecting via a VPN to Sinergia's platform.
- Sinergia do not transfer any personal data to a third-party partner without any prior acceptance from the data controller.
- Sinergia do not transfer data outside of Europe. If in an exceptional case it would have to do so, Sinergia wouldn't proceed without prior acceptance from the data controller.
- Limited access, encryption and regular deletion of data are the main measures that ensure data security

4.3. Legal documentation

Sinergia has a public Privacy Policy available anytime on www.artizan.ma. All legal documentation binding Sinergia and its business partners is also available on the official website.

4.4. Users' rights

Data can be transferred, deleted or modified upon request on request by email to our support team : support@artizan.ma. For deletion and modification operation will be processed with limitations that we keep enough data for our legal obligations (like invoicing data).

5. ORGANIZATIONAL MEASURE

5.1. Data transfer

Technically, data transfer between Sinergia and its clients (or their representatives) is done by :

- https on the platform
- SFTP or FTPS for batch file transfers

5.2. Employee access

Every user id is linked to a individual. Personal computers passwords can be reseted or modified only by habilitated employees in respect of a given procedure.

5.3. Confidentiality

The security and confidentiality with which Sinergia employees must process personal data is described and highlighted in Sinergia's internal regulation as well as in its working contracts. In addition, GDPR training session conducted in Sinergia have been underlying the importance of confidentiality.

5.4. Employee training and awareness

Sinergia has regular training sessions to provide information and organize training sessions on data security, confidentiality best practices and internal procedures. Sinergia has been raising its employees awareness through training modules and live general meetings on the importance of confidentiality in our business and especially in regard of the GDPR.

5.5. Other Policies

Sinergia has arrangements in place with all sub-contractors and third parties to ensure operations are processed with the same level of security that offers Sinergia. All legal documentation binding Sinergia and its business partners can be provided upon request and after getting required validations from the CTO with the necessary limitation of details to ensure privacy of our clients and suppliers.

6. MONITORING AND INCIDENT REPORTING

Sinergia does not have a behavior monitoring process but we keep track of most changes made using the interfaces. External monitoring is done to keep track of key services availability. Alerts are sent to our internal team by email to on-duty employees.

7. Changes to this Security Policy

This Security Policy is effective as of the dateline above and will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately after being posted on our website www.artizan.ma.

We reserve the right to update or change our Security Policy at any time and you should check the latest version periodically. If we make any material changes to this Security Policy, we will notify all our employees and partners by email, or by placing a prominent notice on our website.

-THE END-