KWANKO

SECURITY POLICY

2023

PURPOSE

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

1 ROLES AND RESPONSIBILITIES

1.1 Within Kwanko

Kevin Hatry acts as Kwanko's Security Officer. He can be contacted at security [at] kwanko.com. His responsibilities includes:

- the control and maintenance of all Kwanko'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, Kwanko has nominated a Data Protection Officer (DPO) who can be contacted on gdpr [at] kwanko.com. 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

Claranet is our hosting provider. It's role is to handle the servers hosted in the Equinix data centers. They setup the machines and supervise the hardware.
Equinix is our data center. 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. The technical installations also have access by badge restricted to the employees concerned.

2.2 Storage

- Data are hosted by the IT outsourcing company Claranet (https://www.claranet.com/) within Equinix data centers. More specifically data are stored in PA2 and PA3 data centres of Equinix Paris facility (http://www.equinix.com/services/data-centers-colocation/standards-compliance/#/, search « by location » and select 'Paris' site).
- Data stored by Kwanko's portuguese subsidary are hosted by AWS - Amazon Web Services en Irlande
- Claranet has the ISO 27001 – Information Security certification and the ISO 27701 PIMS (Privacy Information Management System)
- Equinix data centres have the Tier IV Uptime Institute certification level, that is to say, the highest certification possible. Tier IV certification is defined as follow: fault tolerant site infrastructure. Absence of SPOF (Single Point of Failure).
- Access to data center is controlled by Equinix and Claranet. Some Claranet and Equinix employees have physical access to our servers in the datacenter.
- Data is stored in France only.
- Country restrictions can be applied on a per account basis to limit the countries from where a login can be authorized.
- Databases are replicated in two different locations (both managed by Equinix and Claranet).
- Kwanko relies on system level protections: server login is restricted to administrators using SSH keys (no passwords).
- Data at rest is not encrypted.

2.3 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 Kwanko co-workers, clients and suppliers.
- Password complexity rule is a 12 characters minimum and less than 20 characters with numbers, lower case, upper case, special character and no repetition of the same character on more than 50% of the characters. Passwords are hashed using several rounds of sha256 and a random salt.

2.4 Logs and access to logs

- The amount of logged information is too large to be detailed. Kwanko logs all type of information on 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.
- Kwanko business partners can access to logs on request to its CTO. Request will be accepted or not depending on its legitimacy.

2.5 Device security

All Kwanko employees use device protected by Kaspersky antivirus and automatic updates. The hard disks of these devices are encrypted.
Login to personal computers is protected by a password that must respect a minimal length criteria.

3 AUDIT

Kwanko's business partners are welcome to audit Kwanko procedures with the necessary limitation to ensure privacy of our clients and suppliers.
A technical audit of the Kwanko platform is carried out every year by an external company auditor (until 2023: Ernst & Young).

4 DATA

4.1 Personal data

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

4.2 Data accessibility

- Most of personal data Kwanko processes isn't accessible by Kwanko's employees, yet some of it can be. In that case it can be accessible from anywhere in the world by connecting via a VPN to Kwanko's platform.
- Kwanko do not transfer any personal data to a third-party partner without any prior acceptance from the data controller.
- Kwanko do not transfer data outside of the EU. If in an exceptional case it would have to do so, Kwanko 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

Kwanko has a privacy policy for visitors to the www.kwanko.com public site available at all times on the www.kwanko.com website.
The specific legal documentation binding Kwanko and its commercial partners is also available on Kwanko Platform and on request from the DPO at gdpr [at] kwanko.com.

4.4 Users' rights

Data can be transferred, deleted or modified upon request to our DPO (gdpr [at] kwanko.com). For deletion and modification operation will be processed with limitations that we keep enough data for our legal obligations (like invoicing data).

5 ORGANIZATIONAL MEASURES

5.1 Data transfer

Data transfer between Kwanko and its clients (or their representatives) is done by:

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

5.2 Employee access

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

5.3 Confidentiality

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

5.4 Employee training and awareness

Kwanko has its own internal training tool (based on the 360Learning platform) to provide information and organize training sessions on data security, confidentiality best practices and internal procedures.
Kwanko has been raising its employees awareness through training modules and live general meetings on the importance confidentiality has in our business and especially in regard of the GDPR.

5.5 Other Policies

Kwanko has arrangements in place with all sub-contractors and third parties to ensure operations are processed with the same level of security that offers Kwanko.
The legal documentation binding Kwanko and its commercial partners is also available on Kwanko platform and, if necessary, on request by email to gdpr [at] kwanko.com

6 MONITORING AND INCIDENT REPORTING

In addition to development practices designed to avoid any vulnerability on the 'classic' flaws identified by OWASP, Kwanko also has a policy of automatically updating systems for security updates. Our development team also monitors application logs (centralised) to identify abnormal behaviour.
Kwanko keeps 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 Channels and by email to on-duty employees.

7 Business CONTINUITY PLAN

The service continuity plan is defined as the strategy and all the measures planned to guarantee the recovery and continuity of services following a disaster or an event that seriously disrupts normal operations.
Our host, Claranet, monitors hardware (checking internal components and RAID) and the availability of key services.
Kwanko also has external application monitoring which tests key urls;