COMMANDERS ACT

Contractual form

"Data protection measures"

# TOM

## Technical and Organizational Measures

2022

# I. INTRODUCTION

This document lists all measures that we implemented in Commanders Act infrastructure and processes in order to guarantee a high level of security for the data we are in charge.

# II. PHYSICAL ACCESS

Our infrastructure is hosted by Amazon Web Services.
All servers containing Data are hosted on the French Region (eu-west-3). AWS provides a high level of security for their datacenters.
For more information see here: https://aws.amazon.com/compliance/data-center/controls/

Hosting is also possible in Equinix Datacenters France (optional and subject to invoicing).

# III. SYSTEM ACCESS

Our servers can only be accessed by employees of Claranet and Commanders Act IT team.

Claranet being our infrastructure manager, they have access to the infrastructure via a secure management network.

Commanders Act employees who have access to the infrastructure can only login via VPN or restricted IP.

Security of system access is provided by:

- Automatic time-out of user
- Continuously monitoring infrastructure security
- Role-based access control implemented in a manner consistent with principle of least privilege
- Access to host servers, applications, databases, routers, switches, etc., is logged
- Passwords must adhere to these rules :
    - Minimum length of 10 characters, and at least one special character
    - Renewal of password every 3 months
- Regularly examining security risks by internal employees and third party auditors
- Issuing and safeguarding of identification codes

# IV. DATA ACCESS AND DATA INPUT

Our customers' data are stored in shared databases with a logical separation.

Besides the administrator accesses covered by the previous chapter, data can only be accessed through our web-based interface, at https://app.commandersact.com

Security for data access is provided by:

- Individual access granted by email verification
- Password policy:
    - At least 9 characters
    - At least 1 number
    - At least 1 capital character
    - At least 1 special character
    - Different from the last 10 passwords
    - Renewal every 3 months maximum
- Differentiated access rights
- All accesses are logged
- All modifications are logged
- Data deletion is logical (for deletable data via the interface)
- WAF (Cloudflare)

All forms in our interface are protected against CSRF attacks.

Our products offer the possibility to make collected data pseudonymous. We can for instance obfuscate IP addresses or encrypt personal data (SHA256 algorithm)

# V. DATA TRANSFER

Our platform is meant to collect and send data. We have implemented different ways of communication between our infrastructure and external assets. Data can be transferred via:

- Web data collection (http hits)
- API
- FTP/SFTP

Data should never be transferred by e-mail or physical medias unless specific recommendation of a customer.

Data transfer security level depends on the Data. Different levels of security can be applied and cumulated.

Security of data transfer is provided by:

- Encryption of critical data
- Tunneling (VPN)
- Transport Security (SSL, IP restriction)
- Data control (checksum)

- Logging

# VI. DATA AVAILABILITY

Our platform is designed to offer high availability of service, data availability included.

Data availability is provided by:

- Redundancy of servers and redundancy of hard drives (RAID technology)
- Dual building infrastructure
- Uninterruptible power supply (UPS)
- Multiple internet connections
- Secured network (Firewall)
- Backup procedures up to one month retention
- Software exclusion, single task servers

Our infrastructure is designed for scalability. All data collection services are scalable and most of them are now auto-scalable. Meaning that the number of servers automatically varies depending on the incoming traffic.

Our infrastructure is also completely industrialized. We use Terraform and Ansible to deploy our infrastructure. In case of emergency we can easily deploy our services anywhere and have the minimum service interruption possible.

# VII. DATA ISOLATION

The data we store and process is the property of our customers. Our infrastructure is designed to prevent leaks and to assure that the data is processed according to its mean.

Data isolation is provided by:

- Internal client concept called “site”
- Database isolation
- Separation of production and development environment
- Separation of production and test data

# VIII. CONTACT

Samuel Font – CIO
samuel.font@commandersact.com
+33 6 26 01 69 89