

Security @ Klaro Cards

Confidential - Version 2025-11-21

An actionable overview of security measures used at Klaro Cards and Enspirit, for an intelligible continuous improvement process with our best customers.

Version 3.1 - 2025

- Added the Service & Data Agreement section for an overview of our obligations.

Version 3.0 - 2023

- Rewrite listed security measures using the Cyber Fundamentals framework's categories.

Version 2.0 - 2020

- Adaptations following the migration from OVH to Google Cloud Services.

Version 1.0 - 2018

- Documentation of usual Enspirit practices related to Cybersecurity
- Backup policy used with OVH servers

Introduction

This document provides an intelligible overview for Klaro Cards customers who want to manage their digital & cybersecurity risks, and/or enter an continuous integration process with Klaro Cards with respect to them.

It answers most frequently asked questions regarding risks & cybersecurity, in layman terms.

Table of contents

Introduction	2
Table of contents	2
Overview	3
Service Level & Data Agreements	4
Security Measures @ Klaro Cards	5
<i>How do we IDENTIFY security issues and threats ?</i>	5
<i>How do we PROTECT our users and their hosted data ?</i>	5
<i>How do we DETECT security issues at runtime ?</i>	7
<i>How do we RESPOND to & RECOVER from security or down time issues ?</i>	7
Any question ? Let's talk !	8

Overview

Klaro Cards is a Belgian company offering a Software as a Service (SaaS) supported digitalisation consultancy service. The software is deployed in two different settings :

- A public cloud instance, where anyone can create an account and start playing with Klaro Cards.
- A dedicated cloud instance, dedicated to a particular customer who signs a specific service level agreement contract (SLA).

Both settings rely on the exact same code base, team, and third party dependencies. The public cloud instance always runs the latest version of the software. Customers asking for their own instance may choose a dedicated deployment policy as part of the SLA.

Klaro Cards relies exclusively on Enspirit SRL (main shareholder, Belgian company too) for the software development and hosting of the SaaS solution. Unless stated otherwise in the customer SLA, the solution is hosted using Kubernetes on Google Cloud Services (GCS), with a Kubernetes cluster, a PostgreSQL database and a storage bucket managed by GCS themselves, with adequate backup policies.

Except Google, the sole persons having a direct access to the hosting servers and customers data are Klaro Cards' CTO (Bernard Lambeau) and Enspirit's CTO (Louis Lambeau). These accesses are only and exclusively used for maintenance and customer support. The only other access to customer data occurs during customer sessions in the SaaS itself, on customer's own invitation.

Klaro Cards and Enspirit SRL are not yet formally compliant to ISO27001, ISO9001, or similar. However they both apply best cybersecurity practices based on a very good understanding of cybersecurity related frameworks (ISO27001, NIS2, Cyber-fundamentals, OWASP, etc.). The sections later in this document lists our security measures using Cyber-fundamentals' intelligible categories.

Both companies and their personal (employees and contractual freelancers) make a continuous attention to Excellence in Software Engineering and Cybersecurity, and are open to continuous improvement processes.

The following section lists improvements that are considered the most important to improve the security of your Klaro Cards instance as a customer.

Service Level & Data Agreements

When you buy a dedicated Klaro Cards cloud instance, we sign two important documents :

- A Service Level Agreement, that covers our obligations regarding the availability of the Klaro Cards SaaS, backups policies, and support reactivity.
- A Data Processing Agreement, that covers our obligations and those of our partners regarding the hosting and use of the data you put in Klaro Cards.

Here is an overview of the default setup proposed, that can of course be fine-tuned for you :

- Klaro Cards makes a best effort to offer 99.5% availability of the SaaS (less than 1 day of downtime per year, cumulated). Since 2019, we were close to 99.9% in practice. That said, our SaaS is deployed in a single Google Cloud zone, without high availability. This may be fine-tuned of course..
- Dedicated cloud instances always run a stable version, that has been battle tested on the public cloud version of the SaaS first. We upgrade dedicated instances once a month approximately, to run the latest stable version (urgent security fixes may force intermediary upgrades).
- Klaro Cards performs data backups on a daily basis and keep previous backups during 30 days. Hence, the maximum data lost in case of disaster is 24h. In case of a disaster, Klaro must restore the availability on the last available data backup within 3 business days.
- Klaro Cards strictly limits its own use of your own data. This applies to the personal data (about your users) and everything you put into your Klaro Cards cards, boards, projects, etc. We never sell or share your data with third parties, unless its strictly required to guarantee our SaaS service (e.g. hosting, support & maintenance, communication), etc.
- All our data processing subcontractors (e.g. Enspirit, Google Cloud, Odoo) have signed a Data Processing Agreement with strict obligations with respect to data privacy and data breach reporting.
- Our support team guarantees a maximum response time of 6h (open hours only) for severe blocking bugs involving all users. We make a best effort to answer all requests within 24h otherwise, with a strict 8 business days commitment.

Security Measures @ Klaro Cards

This sections and subsections lists current security measures used at Klaro Cards to ensure correct data management & cyber security in the best possible way. The section is organised following the sections of the Cyber Fundamentals framework (by Belgium's Cyber Security Coalition).

How do we IDENTIFY security issues and threats ?

Asset management

- Klaro Cards's physical assets is kept as minimal as possible and relies on professional cloud offering by Google Cloud Services, applying security best practices documented by Google.

Governance

- Klaro Cards & Enspirit rely on a very good knowledge of the Cyberfundamental (NIS2) security frameworks, GDPR, and 21CFR (Part 11). This knowledge drives product decisions, daily practices and training of personnel where applicable.
- Cybersecurity issues, found by Enspirit's technical team, external security hackers (bug bounty program) and penetration testers (on mission), are managed, evaluated and worked on in a continuous way like other features or bugs.
- The CTOs and key technical personal of both companies are registered to relevant security newsletters and share information immediately when any issue might impact our software & deployments.

Risk assessment

- Software vulnerabilities and threats are actively looked for and monitored, using dedicated SaaS solutions (Aikido.dev), manual penetration testing (bug bounty program, Cresco Cybersecurity), and proactive unhappy path testing..

How do we PROTECT our users and their hosted data ?

Awareness and Training

- Klaro Cards is developed by a senior and stable technical team at Enspirit. Junior software developers never commit code that is not reviewed. Every feature is taken as an opportunity for the team to share best practices.
- Senior engineers are in continuous contact with ethical hackers as part our bug bounty program. This allows them to keep being aware of the most recent security issues.

- All developers working on Klaro Cards, as well as non technical profiles (e.g. customer support team) are aware of standard cybersecurity hygiene measures (2FA, password policy, phishing, etc.).

Data Security

- Our internal policies forbid production data to be used outside of production environments. In the very rare cases where production data must be copied during maintenance or support, all copies must be deleted immediately after having been used.
- Staging & production environments enforce encryption of all external communications, via systematic usage of HTTPS/SSL.
- All backups are properly encrypted ; encryption keys are securely kept, as per our secrets management policy (see below).
- Data processing agreements are correctly signed between Klaro Cards and all its subcontractors (notably Enspirit & Google Cloud) . Those agreements apply data protection clauses, covering the usage, hosting, and deletion of data, as well as the necessary information & reaction requirements in case of data leakage.

Identity Management

- Klaro Cards and Enspirit both apply a very strict secrets policy. The latter a) imposes the use of 1Password for all secrets, b) requires infrastructure credentials to be kept in dedicated vaults, c) forbids reusing passwords across services, d) forbids sharing secrets without an appropriate sharing solution (limiting the number of accesses and period where the secret is made available).
- Klaro Cards and Enspirit both rely on Google Workspace for identity management of all personal (employees and freelancers). Multi-Factor authentication is enforced on all Google Accounts.
- All critical systems involved in Klaro Cards' development (e.g. Gitlab, Jenkins, Aikido.dev, etc.) are connected to Google's Single Sign On solution.
- Only selected developers of Enspirit have access to Klaro Cards' source code and hosting platforms and these accesses are periodically reviewed.
- Only Klaro Cards's CTO and Enspirit's CTO may release and deploy a new version of the software on a customer dedicated instance and are properly trained to do it safely.

Maintenance and anti-Intrusion

- Software vulnerabilities and threats are actively looked for and monitored (see Risk Assessment earlier).

- A best effort is made to avoid ruining Docker containers as root where possible.
- Web & OWASP countermeasures are applied as extensively as possible, notably HTTP security headers that help preventing and reducing the impact of intrusions and code injection (CSP).
- A continuous attention is made to the systematic upgrade of all software components used inside Klaro Cards (dependencies), on development tools (e.g. Jenkins, Gitlab), and developer computers (e.g. operating systems).

How do we DETECT security issues at runtime ?

Anomalies and events

- Data processing agreements aforementioned impose the use of proper anti-virus and anti-malware measures on developer computers. We rely on Google's own security measures on this aspect in production environments.
- Production environments are monitored both internally and externally (via InternetVista). Alerts reach CTOs via chat systems and SMS in case of an unexpected down time or performance issue.
- Rate limiting mechanisms are enabled on all sensitive Klaro Cards' API endpoints, notably authentication mechanisms and API endpoints sending emails to end users.

How do we RESPOND to & RECOVER from security or down time issues ?

- CTOs of Klaro Cards and Enspirit are in very close continuous contact and used to respond to urgent situations requiring their full technical attention.
- Continuous backups are made, using Google Cloud Service's own backup system of the SQL database used by Klaro Cards.
- A disaster recovery procedure exists that relies on a modern software continuous & integration chain. The latter allows building and deploying the whole SaaS solution from scratch in only a few hours, starting from a standard SQL backup.
- The disaster recovery procedure is very close to the provision of a new Klaro Cards dedicated instance. The latter is ran several times a year, for new customers, and as part of major upgrades during maintenance windows.
- During a crisis, Klaro Cards' simple architecture allow our CTO to run the entire software on a modern developer computer based on a single SQL backup. This allows answering urgent questions that might arise at customer's site during the crisis.

Any question ? Let's talk !

Bernard Lambeau

Co-founder

bernard@klaro.cards

+32 477 24 58 61

Marc Baudy

Business Developer

marc@klaro.cards

+33 6 79 71 93 50