

Quable

Technical & Organisational Measures for Information Security & Data Protection (TOM)

Version:	1.0
Date of version:	09/23/2026
Document owner:	Charly Goblet (Head of Engineering)
Confidentiality level:	Restricted

Change history

Date	Version	Created by	Description of change
2-Mar-2026	1.0	Charly Goblet	Initial version

Table of content

Introduction	6
What is Quable?	6
Why this document?	6
Audience of the document?	6
How to use the document?	6
Information Security Management System (ISMS)	7
Organization of information Security	8
Policies and Procedures	8
Roles and Responssibilities	8
Risk Management	9
Risk Management Methodology	9
Human Resource Security	10
Candidate selection and Screening	10
Onboarding process	10
Offboarding process	10
Confidentiality Clause in Employments Contracts	10
Asset management	11
Asset Inventory	11
Information Classification	11
Access control	11
Quable's Access Control Policy	11
Quable's Password Policy	11
Quable's Manager Password Policy	11
Single Sign-On (SSO)	12
Segregation of duty	12
Least access privilege	12
Onboarding, offboarding, change of position & periodical reviews	12
Multi-tenant and Segregation of data	13
Cryptography	14
Encryption of data at rest	14
Encryption of data in transit	15
Physical and Environmental Security	15
Data processing facilities	15
Quable's Offices	15
Quable's laptops	16
Hard drive encryption	16
Software updates	16
Clear screen, device locking and unattended devices	16
Operations Security	17
Backup Policy	17

Backup of databases	17
Backup of User Provided Content hosted by Quable	17
Emails	18
Application code	18
DDoS and Firewalls	18
Logging & Monitoring	18
Remote access control	18
Communications security	19
HTTPS and SSL	19
Information Systems Acquisition Development and Maintenance	20
Secure Development Lifecycle (SDLC)	20
Features	20
Bugs	20
Teams	20
Development practices	21
Separation of environments	21
Environment accesses	21
High level architecture	22
Code review & Testing	22
Peer Code Review	22
Testing	23
Release Management	23
What is Release Management?	23
Objectives	23
Policies	24
Release Workflow	24
Lesson Learned	24
Production Data	25
Information Incident Management	25
Incident Management Procedure	25
Customer Support	25
Status Page	25
Online assistance	25
Business Continuity & Disaster Recovery	25
Redundancy	25
Business Continuity	26
RTO	26
RPO	26
Disaster Recovery	26
Compliance	27
Security Audits & Reports	27
External audits	27
Penetration test	27
Customers on-demand audits	27

Internal audits	27
Vulnerability scan	27
Artificial intelligence and Compliance	28

Introduction

What is Quable?

Quable SAS is a company providing a PIM/DAM (Product Information Management/Digital Asset Management) solution through SaaS.

Quable is designed to be an integral part of its clients' data ecosystem. It integrates with other corporate IT tools.

Why this document?

This document describes the Technical and Organisational Measures (TOMs) implemented by Quable to ensure an appropriate level of security and data protection across its information systems and services.

It is intended to demonstrate Quable's commitment to protecting the confidentiality, integrity, and availability of information assets, including personal data processed on behalf of its customers and in the context of its own business operations.

This document is structured in accordance with the ISO/IEC 27001:2022 standard, which Quable uses as a reference framework for its information security practices. Quable does not currently hold ISO 27001 certification but applies its principles as the basis for its security program.

Audience of the document?

This document is intended for 3rd party risk assessors, security departments, information security auditors, CISO, or IT departments of prospects, customers, integrators and suppliers.

How to use the document?

The document is structured to follow the domains of the ISO27701 framework and provide excerpts from our internal policies that are declassified for use by the intended audience outside our organisation.

Information Security Management System (ISMS)

An Information Security Management System (ISMS) is a systematic framework of policies, processes, and controls designed to manage and protect an organisation's information assets. It provides a structured approach to identifying security risks and implementing appropriate controls to address them.

Quable has established an ISMS that reflects the size and nature of its operations as a SaaS company. While Quable does not currently hold formal ISO 27001 certification, the structure and content of this TOM and the controls described within it are broadly aligned with the ISO/IEC 27001:2022 standard.

Quable's ISMS is built on the following principles:

- Confidentiality: Customer data and internal information are protected from unauthorised access.
- Integrity: Data is accurate, complete, and protected from unauthorised modification.
- Availability: Systems and data are available to authorised users when needed, in line with agreed service levels.

Information security at Quable is a shared responsibility across Engineering and Management. Security considerations are embedded into day-to-day operations, product development, and business decisions rather than being siloed within a dedicated security function.

Quable is committed to continuously improving its security posture. Controls and policies are reviewed periodically and updated in response to changes in the threat landscape, business context, and customer requirements.

Organization of information Security

Policies and Procedures

Quable maintains a set of internal policies and procedures that govern information security across the organisation. These policies are documented, communicated to all relevant staff, and reviewed on a regular basis. Key policies include:

- Information Security Policy
- Access Control Policy
- Password Policy
- Acceptable Use Policy
- Incident Management Procedure
- Backup Policy
- Secure Development Lifecycle (SDLC) Policy
- Business Continuity and Disaster Recovery Plan

Policies are owned by Engineering and Management and are maintained as living documents. Staff are made aware of relevant policies during onboarding and through periodic communication.

Roles and Responsibilities

Information security responsibilities at Quable are distributed across Engineering and Management, without a dedicated CISO role. The following responsibilities are defined:

Role	Security Responsibilities
Management (VP)	Overall accountability for information security; approval of security policies; risk acceptance decisions.
Engineering Team (Engineering)	Technical security controls; secure development practices; infrastructure security; incident response.
All Employees	Adherence to security policies; reporting of security incidents and suspicious activity; protection of company and customer data.
HR	Security aspects of onboarding and offboarding;

	confidentiality agreements; background checks.
--	--

Risk Management

Risk Management Methodology

Quable recognises that risk management is a foundational element of any effective information security programme. While Quable's risk management approach is not yet formalised through a dedicated risk register or annual risk assessment cycle, risk considerations are actively embedded in how the Engineering and Management teams make decisions.

In practice, risks are identified and addressed through the following mechanisms:

- Security considerations are included in the design and review of new features and infrastructure changes.
- Operational risks — such as availability, data loss, and access control failures — are addressed through technical controls including backups, monitoring, redundancy, and access reviews.
- Supplier and third-party risks are considered when selecting vendors and cloud service providers, with a preference for established providers with strong security track records (e.g. Microsoft Azure).
- Incident reviews are used to identify recurring risks and drive remediation.

Quable is committed to progressively formalising its risk management approach. This includes plans to establish a documented risk assessment methodology, maintain a risk register, and define a clear risk acceptance framework as the organisation grows.

In the interim, the following risk categories are actively monitored and controlled:

Risk Category	Example Threats	Key Controls
Data confidentiality	Unauthorised access, data leakage	Access control, encryption, MFA
Availability	Service outages, DDoS attacks	Redundancy, DDoS

		protection, monitoring
Data integrity	Accidental or malicious data corruption	Backups, audit logs, code review
Insider threat	Employees abusing access rights	Least privilege, offboarding process, access reviews
Third-party risk	Vendor compromise or failure	Due diligence, Azure SLA, dependency monitoring

Human Resource Security

Candidate selection and Screening

Quable's staff is selected through a screening process where their skills and adherence to the culture of the company are assessed.

Onboarding process

Each member of the staff is following an onboarding process during which he/she attends onboarding meetings with a representative of each team. During those meetings the role of the team, their daily tasks and challenges will be discussed so that the new staff member knows the product and the persons behind it.

Offboarding process

Each leaver of the company will follow an offboarding process to ensure that every asset and user access are deprovisioned or returned to the company.

Confidentiality Clause in Employments Contracts

All our employment contracts include mandatory confidentiality clauses in accordance with GDPR.

Asset management

Asset Inventory

Quable's assets are logged into an asset inventory with the assignment of an owner.

Information Classification

The current information classifications used by Quable are:

- Public
- Business use only
- Confidential

Access control

Quable's Access Control Policy

User administrators have real time access to the list of their users and can upgrade/downgrade rights & access. Details of user rights are available here :

<https://docs.quable.com/v5-EN/docs/permissions-reference>

Quable's Password Policy

Quable's Manager Password Policy

- All passwords are chosen by the user, encrypted in transit and stored as a hash at rest in our systems (see [Cryptography](#))
- Password complexity: password must meet all the following requirements:
 - At least 12 characters long
 - At least 1 number
 - At least one special character
- Reset password:

- Password reset link is sent via email
- Session timeout:
 - Back-office sessions last for 30 days (which is prolonged by any action performed on the interface)

Single Sign-On (SSO)

Single Sign-On is available with the main identity providers:

- Google (Social SSO)
- Microsoft (Social SSO)

We also support the following single sign-on protocols:

- Security Assertion Markup Language (SAML)

Segregation of duty

Only a set of Quable employees have access to customer data:

- Helpdesk
- Head of Product
- Solution Architects

Least access privilege

Quable staff members are provided with the minimal access required to perform their duty.

Onboarding, offboarding, change of position & periodical reviews

Accesses are reviewed annually by asset owners in order to verify the proper access level is correctly enforced.

Multi-tenant and Segregation of data

Quable's platform, as a multi-tenant solution, is handling data from different customers. Each customer's data is separated from the other to ensure the isolation of each Quable's customer.

This segregation may be based on:

- Physical segregation (i.e. different physical servers)
- Virtual segregation (i.e. different virtual servers)
- Database segregation (i.e. different databases)
- Database sharding (i.e. partial database segregation)
- Logical segregation (i.e. application level segregation)

In some cases, these methods can also be combined.

The segregation method is selected by Quable based on technical constraints, availability requirement, scalability needs and sensitivity of the data and cannot be selected nor modified by the client.

Cryptography

The following requirements for cryptography have been defined:

- Production servers (Netherlands)
 - In transit: encrypted
 - Encryption algorithm: at minimum AES-128
 - At rest:
 - Filesystems: Every server containing personal data have their filesystem encrypted
- Backup locations (OVH)
 - In transit: at minimum AES-128
 - At rest: Filesystems have their filesystems encrypted
- Sensitive data (API keys, SSO configuration variables...): Encrypted with AES-256 with a key provided at deployment time
- Access to production servers: SSH Private Key is mandatory in order to get access to production servers. These accesses are limited to a subset of Quable staff based on a “need to know” and “least access privilege” principles
- User passwords are hashed using SHA-1 and salt
- Only trusted and non-compromised certificate authority (CA) are used for production purpose
- The creation, distribution, storage and deletion of certificates is strictly managed by the IT top management, or automatically (programmatically) setup under his supervision.

Encryption of data at rest

The following table summarises the encryption at rest in our infrastructure and key management

Name	Company HQ	Datacenter location	Transferred PII's	Encryption at rest	Encryption key owner
Azure	USA	EU		Y (HDD level)	Azure
OVH	France	EU	Backup of customer data	Y (S3 level)	OVH

Encryption of data in transit

From To	Azure	OVH	CND77
Azure		TLS	TLS
OVH	TLS		TLS
CDN77	TLS	TLS	

Physical and Environmental Security

Data processing facilities

Our core-business applications are located inside datacenters of Azure (Microsoft) located in the Netherlands and OVHCloud located in France, which are ISO27001 and SOC2 compliant, ensuring the use of:

- Strict visitor policy
- Alarm system
- Video surveillance equipment (CCTV)
- Fire prevention
- Climate control systems
- Redundancy of power and telecommunication supplies
- ...

Quable's Offices

- Access to our offices is secured
- Offices are locked outside of office hours
- No data is hosted in our offices

Quable's laptops

Quable laptops users are required to enforce the following measures :

Hard drive encryption

Windows users must encrypt their hard drive with BitLocker and provide a proof of this activation.

Mac OS users must encrypt their hard drive with FileVault and provide a proof of this activation.

Linux users must encrypt their hard drive with their operating system tools and provide a proof of this activation.

Software updates

Laptops must always be updated to the latest stable version of the software (application and operating system) provided by the editor.

Clear screen, device locking and unattended devices

If the authorised person is not In direct control of the device, all sensitive information must be removed from the screen.

In the case of short absence, the clear screen policy is implemented by locking out of all systems or locking the screen with a password or biometric security (fingerprint). Auto locking rule must be set to lock Mobile Computing Device automatically after a defined period of time.

In the case of longer absence (eg: holidays), the user must log out from his session.

The policy is also ruling the fact that laptops should never be left unattended if not in a secure area.

Operations Security

Backup Policy

The following types of data are part of our Backup policy:

- Databases
- User provided content hosted by Quable
- Email
- Application Code

Backup of databases

Quable's databases host the most sensitive and mission critical information of the company.

For this reason, all databases containing customer data are:

- Backed up
 - Storage is performed on any of Quable EU datacenter (OVH)
 - Retention period is 365 days
- Frequency of backups
 - Backups are performed once per day

Additional backup is also enabled on Azure and performed once per day with a retention period of 1 day.

Backup of User Provided Content hosted by Quable

Content provided by our customers (assets) is stored in Azure EU data centers (object based storage). In addition, this content is also

- Backed up
 - Storage is performed on any of Quable EU datacenter (OVH)
 - Retention period is 7 days
- Frequency of backups
 - Backups are performed once per week

Emails

Our emails are hosted by Google Mail, their backup is ensured by Google.

Application code

Application code is versioned through GIT, backup of the git repository is ensured via regular checkout of the repository.

DDoS and Firewalls

Our infrastructure is protected by network appliances performing load-balancing and rate limiting, only the minimum amount of services are exposed to public network access.

Logging & Monitoring

Quable has put in place adequate tools to log, monitor and alert teams in real-time in case suspicious activity is detected.

System logs are shipped and aggregated in Datadog. Application logs are shipped and aggregated in our own Elasticsearch service. The following platforms are used to support our logging, monitoring and alertings needs:

- Datadog : for system logs, reactive monitoring and alerting
- ELK stack : for application logs
- Squadcast : for on-call management

Remote access control

All our servers are protected against intrusions by exclusive access through a management VPN. SSH access is always based on private-key authentication. Access to servers is done by using a bastion to ensure minimal exposure surface.

All external services are accessed using SSO to ensure limited access to those services on a need to know basis.

Communications security

HTTPS and SSL

Front-end: All customer's domains are only available through HTTPS (HTTP will fallback to HTTPS).

Back-end: All our APIs are only available through HTTPS (HTTP will fallback to HTTPS).

Traffic to end-users is encrypted using TLS 1.2 and 1.3 only.

Cypher suite for TLS 1.2 (by order of preference)

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Cypher suite for TLS 1.3 (by order of preference)

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Information Systems Acquisition Development and Maintenance

Secure Development Lifecycle (SDLC)

Scrum methodology and Kanban frameworks are used in order to drive and manage our developments.

Each request is assigned a type being:

- Features: A new feature for the product available to all our customers
- Bugs: A correction to an existing feature of the product. Bugs also include incidents.

Features

All features are defined using “User Stories” created by the Product owner and submitted to representatives of the development and QA teams.

Features are scheduled into Sprints as soon as they reach the “Ready” state.

Bugs

All bugs are evaluated by the support and a dedicated support development team (PGS) and, based on their criticality, are prioritized in the Kanban of the PGS team.

Teams

We have multiple teams working together to develop, maintain and evolve the Quable software:

- Product team
- Quality Assurance team
- Development teams
- Infrastructure team

Development practices

Quable maintains and operates a single codebase for all of its clients. This code is developed with a strong focus on quality and performance.

Quable tries to avoid big-bang and/or reinventing the wheel. For these reasons Quable is:

- Using continuous integration with automated pipelines
- Using frameworks and components whenever possible
- Evolving existing applications instead of re-starting from scratch
- Documenting architecture decisions using ADR

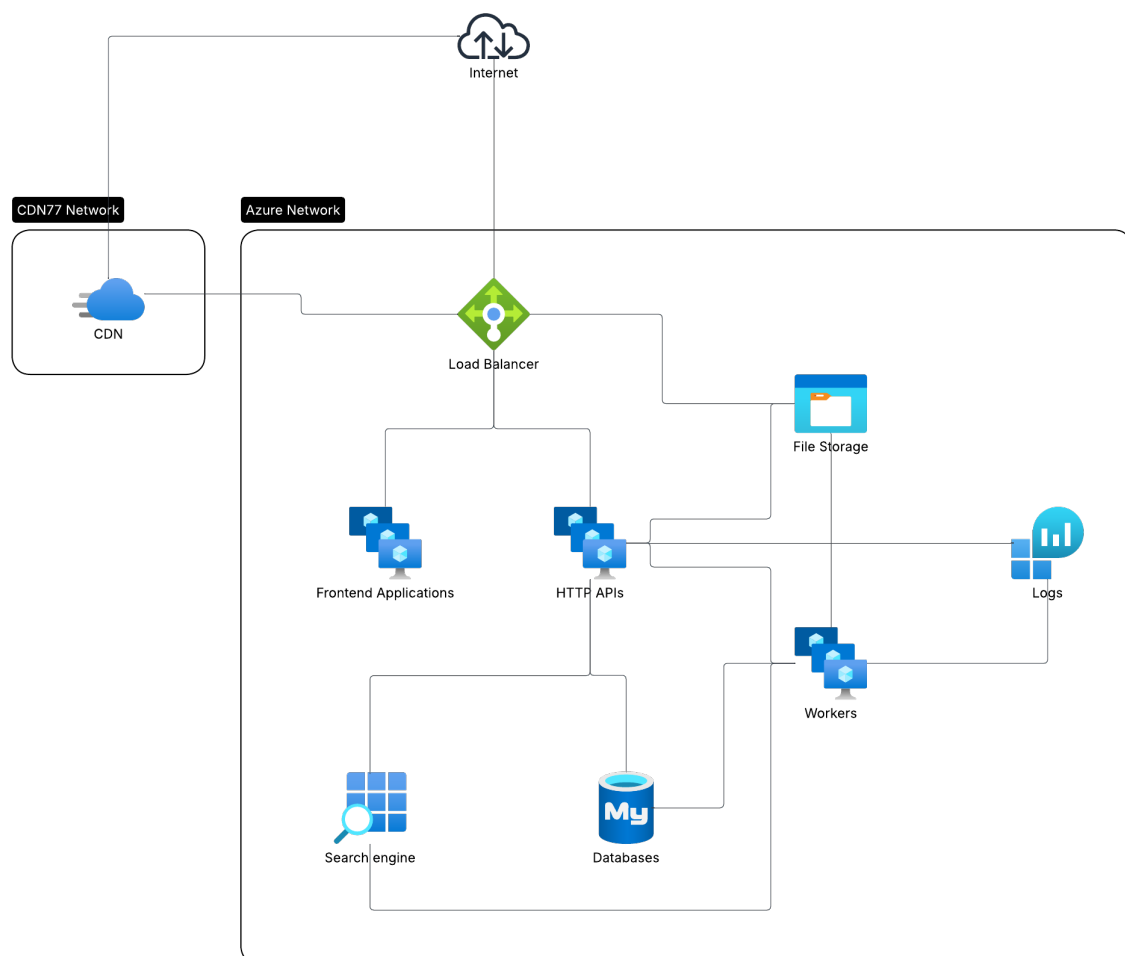
Separation of environments

Environments are separated and only production servers contain real data, developers and testers are working on their respective environments with testing data.

Environment accesses

Quable has different environments, for development, QA and production. Database access is restricted per user. When direct access to the production database is needed for debugging purposes, read only access may be granted to a limited pool of internal users.

High level architecture



Code review & Testing

The technologies we use include the most advanced frameworks and software components: PHP, NodeJS and React.

Peer Code Review

All code ready for production is countersigned by at least 1 other internal developer based on the project.

Testing

Testing is a crucial part of our product development, that's why we have a dedicated QA team internally. Testing is performed manually and automatically.

Quable uses a mix of:

- Unit tests: automated testing at application level
- Integration tests
- End-to-end testing
- Manual regression testing

We make use of automated tests whenever possible through a test platform (like Postman for all API regression tests).

These tests are automatically triggered by our continuous integration platform.

Vulnerability scan

Quable is constantly scanning its infrastructure against open ports or well known vulnerabilities. Peer dependencies in the product's code are also scanned against CVS databases to keep track of outdated dangerous dependencies.

Release Management

What is Release Management?

Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments, including testing and deploying software releases.

Release management ensures that we are delivering new features while protecting the integrity of existing services.

Objectives

- Ensure a high number of successful releases
- Maintain a low number of incidents caused by releases
- Create a single documented process for managing all releases
- Ensure that the process is adopted and escalated to management if there are compliance issues
- Improve productivity by establishing standard release processes and tooling
- Harvest lessons learned from the release management process that could be applied to other areas of service management

Policies

- All changes (a release can contain multiple enhancements or fixes) must go through the release management process with appropriate approvals
- Whenever possible, changes to an existing service should be bundled together and released on a regular basis using the release management process
- Each release should be well tested and verified prior to deployment by our QA team

Release Workflow

- If a downtime is to be expected, a maintenance is scheduled on the status page: <https://status.quable.io/>
- All features/tickets are available in pre-production environments

- All features/tickets are reviewed by QA team in pre-production environments
- All features/tickets are updated with the correct label: Ready for Production
- Pre-production branch is merged into production branch
- Release is correctly tagged
- Release note is added to git tag
- Release communication (internal and external if needed)

Lesson Learned

Each release must have a post analysis on problems we encountered. If a major incident occurs, Quable must be able to provide a post-mortem on demand at a maximum of 15 days after the incident occurred.

In our internal review we gather the following information:

- Description
- Timeline
- Severity
- Impacts
- Workarounds
- Solution to observer for next releases

Production Data

Production data is restricted only to the production environment. Development and testing are performed on dummy test data.

Information Incident Management

Incident Management Procedure

Quable has implemented an Incident Management Procedure. It handles appropriate duties for responding to, mitigating and to remedying incidents.

Maintenance

Quable will inform its customers of upcoming maintenance that may disrupt normal operations. The notification will be issued at least 14 calendar days prior to the maintenance.

Customer Support

Status Page

A status page is available at: <https://status.quable.io/> with the possibility to register for notifications via email, slack, or RSS.

Online assistance

All Quable's users can contact the Helpdesk in-app. The in-app integration also provides information about the current status of in-progress incidents.

Business Continuity & Disaster Recovery

Redundancy

In order to ensure its SLAs, Quable makes use of data centers, all ISO27001 and SOC2 Type II certified.

Business Continuity

Quable has defined business continuity scenarios that respond to disruptions due to environmental, technical or human factors.

These scenarios have been defined to meet the RTO and RPO approved by management.

RTO

RTO (Recovery Time Objective) is the maximum time during which data is unavailable.

All backup solutions deployed in Quable should ensure a RTO of maximum 24h.

RPO

RPO (Recovery Point Objective) is the maximum time since the last backup point. It quantifies the maximum amount of data that can be lost.

The RPO depends of the type of information

- Up to 7 days for binary assets
- 24h for all other data

All the metrics above should apply 99% of time. Due to the way backup works, it is acceptable to have punctual exceptions to these timings.

Disaster Recovery

A disaster recovery procedure has been defined to recover the production systems in case of disaster (recovering from scratch). The disaster recovery applies for all production systems needed to provide the Quable service to our customers. Quable targets complete recovery of the service within a maximum of 7 calendar days from the declaration of the disaster, with a maximum data loss corresponding to the most recent successful backup.

Compliance

Security Audits & Reports

Quable is running periodic assessments on the security of its product, and at least once a year. They are performed by a 3rd party (external audit).

External audits

Penetration test

A penetration test is an authorized simulated cyberattack on Quable's infrastructure and application, performed to evaluate the security of its platform. The test aims to identify vulnerabilities, including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

Quable is contracting with external parties to conduct penetration tests missions once every 2 years.

Customers on-demand audits

Upon written request, Quable allows its customers, or an independent auditor mandated by its customer, to conduct penetration testing or vulnerability assessments of the solution. The scope, dates, methods and target environment of any test shall be agreed in advance with Quable.

Testing shall be limited to the customer's own tenant, shall not affect the availability of the service, and any findings shall be communicated to Quable without delay and treated as confidential.

Artificial intelligence and Compliance

Quable has introduced internally developed AI features to enhance content generation within the PIM. These features utilize the OpenAI API for generating content efficiently and effectively.

AI generated content is opt-in, the customer must configure the product to enable AI capabilities. He will be required to provide which information is sent to the LLM. Data shared with the OpenAI Api is not utilized for training or fine-tuning the AI models. Content generated by AI remains fully editable.