

Qualifio

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

Version:	3.7
Date of version:	11/03/2025
Document owner:	Patrick Nollet (CISO)
Confidentiality level:	Restricted

Change history

Date	Version	Created by	Description of change
27-Sept-2019	1.0	Patrick Nollet	Initial version
08-Jan-2020	1.1	Patrick Nollet	Updated with ISO27701 & pen test calendar, right to audit,USB storage policy and insurances.
08-Apr-2020	1.2	Patrick Nollet	Reviewed structure and content to split ISMS and PIMS topics
16-Sept-2020	1.3	Patrick Nollet	Reviewed subcontractors section + included the eLearning tools
04-Nov-2020	1.4	Patrick Nollet	Added High level architecture + data flow. Refer to Cookie policy + SLA on Security vulnerabilities
01-Dec-2020	1.5	Patrick Nollet	Update on Subcontractor : Zendesk Pod 18
25-Mar-2021	1.6	Patrick Nollet	Updated password strength;list of subcontractors and certifications, DPO, SSO
02-Apr-2021	1.7	Quentin Paquot	Timeframe update on External audits & link to General terms and conditions.
14-Apr-2021	1.8	Patrick Nollet	Reviewed paragraph on PII retention period (access logs added + specific processing IP addresses)
30-Jun-2021	1.9	Patrick Nollet	Review of the incident handling procedure
30-Nov-2021	2.0	Patrick Nollet	Adding Amazon Web Services, Microsoft Azure and Google Workspace as subcontractors
10-Feb-2022	2.1	Patrick Nollet	Added new MFA development + updated application session timeout
18-Mar-2022	2.2	Fabien Tramasure	Added subcontractor's SCC and TIA measure
22-Mar-2022	2.3	Quentin Paquot	Update of the emergency number outside business hours
30-Mar-2022	2.4	Quentin Paquot	Updated SLA's Front/Back for Platinum customers + reference added to General & Specific terms & conditions
26-Apr-2022	2.5	Patrick Nollet	Added precision on ownership and management of cryptographic keys.
09-Aug-2022	2.6	Laurent Mélon	Minor updates, adaptations & rewording
20-Sept-2022	2.7	Patrick Nollet	Added CDN77 as subcontractor + reviewed access control & Laptop policy sections.

14-Feb-2023	2.8	Patrick Nollet	Updated according to backup policy + SLA on incident mitigation + high level architecture
02-May-2023	2.9	Patrick Nollet	Referring to Subcontractors list on public website. Update of the patching policy
22-Aug-2023	3.0	Patrick Nollet	Reviewed encryption and subprocessor sections
19-Mar-2024	3.1	Patrick Nollet	Reviewed PII anonymization and retention period
16-Apr-2024	3.2	Patrick Nollet	Some improvements based on customer feedback
07-May-2024	3.3	Patrick Nollet	Merged segregation of data section with DPA
25-Jun-2024	3.4	Patrick Nollet	Improved section on business continuity and DRP
29-oct-2024	3.5	Laurent Hauben	Added section on consent management
10-dec-2024	3.6	Patrick Nollet	Added section dedicated to the Italian market. Included NIS2 identification
11-Mar-2025	3.7	Patrick Nollet	Reviewed SLA (moved to contractual documentation) + added section about the use of Artificial Intelligence

Table of Content

Introduction	8
What is Qualifio?	8
Why this document?	8
Audience of the document?	8
How to use the document?	9
Information Security Management System (ISMS)	10
Organisation of information Security	10
Policies and Procedures	10
Roles and Responsibilities	10
Risk Management	11
Risk Management Methodology	11
Human Resource Security	11
Candidate selection and Screening	11
Onboarding process	12
Security awareness and continuous education	12
Offboarding process	12
Confidentiality Clause in Employments Contracts	12
Asset management	13
Asset inventory	13
Information Classification	13
Access control	13
Qualifio's Access Control Policy	13
Qualifio's Password Policy	14
Qualifio's Manager Password Policy	14
Single Sign-On (SSO)	15
MFA (Multi-Factor Authentication)	16
Segregation of duty	16
Least access privilege	16
Onboarding, offboarding, change of position & periodical reviews	17
Users accountability	18
Multi-tenant and Segregation of data	18
Cryptography	20
Encryption of data at rest	21
Encryption of data in transit	21
Physical and Environmental Security	22
Data processing facilities	22
Qualifio's Offices	22
Qualifio's laptops	22
Hard drive encryption	23
Antimalware protection	23
Clear screen, device locking and unattended devices	23
USB Mobile Storage Device	23

Operations Security	24
Backup Policy	24
Backup of databases	24
Backup of User Provided Content hosted by Qualifio	25
Documentation & internal files	25
Emails	25
Application code	25
DDoS and Firewalls	25
Logging & Monitoring	25
Remote access control & Intrusion Detection & Prevention	26
Communications security	26
HTTPS and SSL	26
Information Systems Acquisition Development and Maintenance	27
Secure Development Lifecycle (SDLC)	27
Features	27
Bugs	27
Customer projects	28
Teams	28
Development practices	28
Separation of environments	28
Environments accesses	29
High level architecture	30
Data flow & PII lifecycle	31
Code review & Testing	31
Peer Code Review	31
Testing	32
Release Management	32
What is Release Management?	32
Objectives	32
Policies	33
Release Workflow	33
Lesson Learned	34
Production Data	34
Information Incident Management	34
Service Level Agreement	34
Front Office - "Player"	34
Back Office - "Manager"	35
Status Page	35
Customer Support	35
Ticket creation	35
Office Hours	35
Ticket categorization	36
Priority levels	36
Response Time & Incidents handling	37
Incident mitigation	39

Incident remediation	40
Measurement	40
Penalties	40
Technical vulnerabilities management and Patching policy	41
Technical vulnerabilities patching	41
Other patches and updates	41
Major version changes	41
Fair use policy	42
Business Continuity & Disaster Recovery	42
Redundancy	42
Business Continuity	43
RTO	43
RPO	43
Disaster Recovery	44
Compliance	44
Security Audits & Reports	44
External audits	44
Penetration test	44
Customers on-demand Audits	44
Internal audits	45
Vulnerability scan	45
Static Code Analyzer	45
Insurances	45
NIS2	45
Why aren't we ISO 27001 or ISO 27701 certified?	46
Data protection and privacy	46
Qualifio as "data processor"	46
Qualifio's Data Privacy management interface for customers: The GDPR Toolbox	46
PII Retention Policy	48
All PII's except IP addresses	48
IP addresses	48
Data subjects erasure	49
Data subjects export	49
Default data protection/privacy texts	49
GDPR requests	49
GDPR logs	50
Overview of all questions	50
Overview of all identification fields	50
DPO account management	50
Restitution of Data at the end of the contract	50
Qualifio GDPR protection measures documentation	50
Access the GDPR Toolbox via API	51
Consent management and opt-in	51
Organisational measures to ensure security and protection of PII	51
Data Protection Officers	51

Human resource measures	52
Confidentiality clause in employment contracts	52
Security awareness and continuous education of staff	52
Data Breaches procedures	52
Incident intake	52
Assessment of the incident	53
Incident handling	53
Handling the “Security” aspect of the incident	53
Handling the “Privacy” aspect of the incident	53
Incident closure	54
Transfer of PII to the customer	54
Automatically push of PII to customer’s information system	54
Manual transfer of PII to customer	55
Technical measures to ensure security and protection of PII	55
Privacy by design and by default	55
Cookie Management	55
Deletion of PII	55
Restricted access to production Personal Data	56
Physical access to our offices	56
Computers	56
IT security controls	56
Contractual agreements with Customers	57
Data Processing Agreements	57
Records of Processing activities	57
Qualifio’s sub-processors	58
Artificial intelligence and Compliance	59
Specific requirements for the Italian market	61
Introduction	61
Infrastructure	61
Database hosting	62
Drawing of winners	63
Account setup and limitations:	63
Configuration of gifts (before campaign start)	64
Participation (data collection phase)	64
Drawing of winner	65
Annex 1: Definitions	66

Introduction

What is Qualifio?

Qualifio is a company providing leading “engagement and data collection” as well as Loyalty solutions through SaaS. It enables publishers, brands and agencies to easily create and publish viral interactions on websites, mobile apps and social media. Quizzes, polls, tests, animated games, multimedia galleries and other innovative formats allow them to collect data and to engage, grow, monetise, qualify and loyalize their digital audiences.

Qualifio enables editorial, marketing, CRM and sales teams to build and publish a wide array of interactive contents, in record time and at a reduced cost, with no IT knowledge.

Qualifio is designed to be an integral part of its clients' data ecosystem. It easily integrates with other corporate IT tools such as CRM, CMS, e-mailing, Single Sign-On, Analytics, DMP or even payment systems.

Qualifio is perfectly suited for media and brands with multiple brands and users. Along with access to the online platform, it provides a highly responsive help desk, training and best practices workshops, as well as a Studio to build custom campaigns on behalf of clients.

Thanks to its dedication to security, Qualifio has satisfied exigence of the majority of Media Groups (in Benelux, France & Spain, including : DPG Media, Schibsted, Prisma, Mediaaan, Mediahuis, NPO, RTL, Sanoma, France Télévisions, Lagardère, Radio France etc) as well as brands (Pepsico, Nestlé, AG Insurance, Carrefour, Décathlon, Banks, Lotteries, etc..).

Why this document?

This document aims to provide an overview on the Information Security Management System (ISMS) in place within Qualifio. It will help prospects, customers and suppliers to assess the maturity of Qualifio's information security.

Audience of the document?

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

The document has to be read with its annexes that contain definitions, as well as references.

In order to keep the document stable in time, we are using “references” for mutable content. References can be identified in the text by a key written in italic between brackets [*Reference*], the value of the key will be available in the reference table from [Annex 2: References](#).

Information Security Management System (ISMS)

The CISO and DPO are managing respectively the Information Security and Data Protection at Qualifio by running a state-of-art ISMS (Information Security Management System) and PIMS (Personal Information Management System) , following the ISO27701 international standard.

The ISO27701 standard is used as the framework to manage, with a systematic and exhaustive approach the security of information through its lifecycle within Qualifio.

Organisation of information Security

Policies and Procedures

The ISMS and PIMS are composed of a set of Policies, Procedures and Supporting Documents that are created, reviewed and approved by the Management of Qualifio.

The ISMS and the PIMS are communicated to all staff members of Qualifio, and are explicitly part of the contractual agreement of staff members with Qualifio. The contractual agreement is also referring to the disciplinary process in place in case of violation of the ISMS and PIMS.

Moreover, the ISMS and PIMS are part of the awareness program provided to all staff members of Qualifio

Roles and Responsibilities

Information Security is managed at Qualifio by its CISO (Chief Information Security Officer), directly reporting to the CEO (Chief Executive Officer).

A DPO (Data Protection Officer) has been appointed by Qualifio to answer questions related to the protection of PII (Personally Identifiable Information).

These responsibilities are spread over multiple persons in order to provide a clear segregation of duty while operating the ISMS and PIMS.

Qualifio policies are approved by Senior Management of Qualifio for their adherence to the company's strategy before being rolled out to the company.

Risk Management

Risk Management Methodology

The risk management methodology run by Qualifio is evaluating risks based on the impact if a risk is getting real, and the likelihood of its realisation. Both, impact and likelihood, are scored on a scale of 1 to 5. The final score of a risk is then evaluated by multiplying its impact by its likelihood.

A risk appetite is defined with Senior Management and risk above the risk appetite are treated.

The possible treatments of a risk are:

- **Mitigation:** Selection of security control or controls from Annex A of the ISO/IEC 27001 standard or some other security controls
- **Transfer:** Transferring the risks to a third party – e.g. by purchasing an insurance policy or signing a contract with suppliers or partners
- **Avoidance:** Avoiding the risk by discontinuing a business activity that causes such risk
- **Acceptance:** Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialise

The risk register is owned by the CISO and is reviewed yearly. The risk appetite is decreased at each iteration of the risk assessment.

Human Resource Security

Candidate selection and Screening

Qualifio'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 is following training (up to 10 weeks) in order to ensure that the resource has the skills needed to perform the job. The learning curve is assessed weekly with the manager and a "Qualifio buddy" (internal mentor to help the new hire in its learning curve) that is assigned at the hiring of the person.

A final assessment is performed at the end of the onboarding process of the new-hired in order to verify the knowledge of the person on the product and the process within the company.

Security awareness and continuous education

Qualifio has deployed a training and awareness program towards its staff.

Training and awareness sessions are performed

- On person: through ad hoc training for limited audience or during our "General company meetings" performed 2 times a year for global audience
- Online: through an eLearning platform to deploy training campaign along the year

Specific attention is given to data protection and privacy through:

- Recurrent training sessions regarding Security and Privacy provided by the CISO, DPO or legal team
- Specific GDPR and security workshops for developers & product managers;
- GDPR omnipresent in our content marketing, including via quizzes & tests;
 - Ongoing sensibilization via our internal communication platforms
 - The services of a seconded lawyer.

Offboarding process

Each leaver of the company will follow a strict offboarding process to ensure, thanks to the asset and user access inventories, 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

Qualifio's assets as well as 3rd party assets on which the company depends on are assessed once a year. All assets are logged into an asset inventory with the assignment of an owner and the classification of the asset based on its criticality for the company.

The responsibility for the asset inventory and its annual review is the responsibility of the CISO.

Information Classification

A formal Information Classification has been crystallised into a policy ruling, the classification of information, its owner, its treatment, handling procedures, disposal and destruction.

The current information classifications used by Qualifio are:

- Public
- Business use only
- Confidential

Access control

Qualifio'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://qualifio.zendesk.com/hc/en-us/articles/201717117-What-are-the-different-user-status-and-what-rights-do-they-grant->

- Engage module
 - Administrator
 - Marketer

- Editor
 - External user
 - Observer
- Loyalty module
 - Administrator
 - Designer
 - Editor
 - Observer
- For accounts on the manager module
 - One user per email address.
 - An expiry date of an account can be scheduled (on Engage module only)
 - There is a functionality available to manually disable user accounts
 - User accounts are disabled after 365 days of inactivity.
- For end-users on the loyalty module
 - One user per email address
 - End-user can optionally link their identity with their social media account
 - One default role for all end-user accounts
 - There is a functionality available to manually block end-user accounts

Qualifio's Password Policy

Qualifio'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 1 capital letter
 - at least 1 small letter
 - at least 1 special character
- Password history:
 - Users cannot reuse their previous 100 passwords (hashed version of all previous passwords are kept in database)
- Password expiration:
 - Password expires after 90 days

- Brute force protection
 - After 10 wrong attempts, a one minute delay is required before the next attempt
 - Each subsequent wrong attempt increase this delay by 1 minute
 - The delay is increased up to a maximum of 15 minutes
 - The number of wrong attempts is reset after 12 hours
- User creation:
 - Invitation is sent by email to the user
 - Link is available for 7 days
 - If the user hasn't logged in after the link has expired, the user must start a reset password procedure
- Reset password:
 - Password reset link is sent via email
 - Temporary: link available for 1 hours
- Temporary password:
 - In case the 'Reset or invitation email' is not received by the user, a temporary password can be generated by the support team and sent to the user
 - The user will need to create a new password on the first login
- Password caching is not allowed
- Session timeout: Back-office sessions last for 45 minutes (which is prolonged by any action performed on the interface eg: click, mouse moved, content edited, etc.)

Single Sign-On (SSO)

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

- Google (Social SSO)
- Microsoft (Azure Active Directory)

We support as well the following single sign-on protocols:

- OAuth (specifically OAuth 2.0 nowadays)
- OpenID Connect (OIDC)
- Security Assertion Markup Language (SAML)

This solution provides flexibility to our customers to easily comply with their own secure authentication requirements and policies.

MFA (Multi-Factor Authentication)

Qualifio provides a two-factor authentication (2FA) method using a time-based one-time password. This security layer is deactivated by default and can be turned on to re-enforce security.

Admins can enforce the usage of the 2FA:

- Per user
- For the whole account

The time-based one-time password authentication applications supported are FreeOTP and Google Authenticator. The link between the device and the account can be reset by the Admins in the back-office. Once enabled, the 2FA connection is mandatory for every login.

The 2FA can be used with the email-password or the SSO method.

Qualifio strongly recommends their users to use the multi-factor authentication provided through the integration with their Identity Provider (see Single Sign-On).

Segregation of duty

Qualifio has implemented internal technical processes to restrict sales staff to access client's campaigns reporting and CRM. Only a set of Qualifio employees have access to the export of customer data:

- Helpdesk Manager
- Head of Product
- DPO

Least access privilege

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

Onboarding, offboarding, change of position & periodical reviews

Organisational processes are in place to control the provisioning and deprovisioning in case a staff member is joining, or leaving, or changing his/her position in the organisation.

Accesses are reviewed periodically by asset owners in order to verify the accuracy of accesses to their assets.

Users accountability

Engage logs all actions that have a GDPR impact in the GDPR Toolbox for DPO's (deleting data, access to statistics, etc.)

Logs GDPR

User

All

Actions performed between the

17

1

2018

and the

18

1

2019

Actions

All

Search

Date	User	Action
10/01/2019 - 14:22:37	1751 - Quentin [redacted] [redacted]@qualifio.com	Exported the statistics of the following campaign: Campaign [redacted] (487010)
10/01/2019 - 14:21:39	1751 - Quentin [redacted] [redacted]@qualifio.com	Consulted the data of the following campaign: Campaign [redacted] (487010)
10/01/2019 - 14:21:37	1751 - Quentin [redacted] [redacted]@qualifio.com	Consulted the data of the following campaign: Campaign [redacted] (487010)
07/01/2019 - 13:30:59	6446 - Sophie [redacted] [redacted]@qualifio.com	Consulted the data of the following campaign: Campaign [redacted] (487492)
07/01/2019 - 13:30:58	6446 - Sophie [redacted] [redacted]@qualifio.com	Consulted the data of the following campaign: Campaign [redacted] (487492)
27/12/2018 - 13:49:00	1751 - Quentin [redacted] [redacted]@qualifio.com	Consulted the data of the following campaign: Campaign [redacted]

Close

Export

Multi-tenant and Segregation of data

Qualifio's platform, as a multi-tenant solution, handling data from different customers. Each customer's data is separated from the other by a strict "chinese wall" that ensures the isolation of each Qualifio's customer.

This segregation may be based on:

Technical & Organization Measures for
Information Security & Data Protection

v3.7

18/60

- 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 (e.g. Database sharding and logical segregation).

The segregation method is selected by Qualifio based on technical constraints, availability requirement, scalability needs and sensitivity of the data and cannot be selected or modified by the client.

The testing of the “chinese wall” principle is ensured through extensive regression testing for each release of the Qualifio’s solution.

Cryptography

The following requirements for cryptography have been defined:

- Production servers (Roubaix, Gravelines, Strasbourg, Frankfurt, Warsaw)
 - In transit : encrypted
 - Encryption algorithm : at minimum AES-256 (cf cipher suite)
 - This encryption algorithm is accepted by [NIST Special Publication 800-52](#)
 - At rest :
 - Filesystems: Every server containing personal data have their filesystem encrypted (Bitlocker solution for Windows based servers, AES-XTS for Linux based servers)
- Backup locations (Roubaix, Gravelines, Strasbourg, Frankfurt, Warsaw)
 - In transit : at minimum AES-256 (cf cipher suite)
 - At rest : Filesystems have their filesystem encrypted with AES-XTS
 - All data can be deleted via manual or automatic rules by DPO within the built-in GDPR Toolbox
- Sensitive data (API keys, SSO configuration Variable,...): Sensitive data are encrypted with AES-256 with a key provided at runtime to the application.
- Access to production servers: SSH Private key is mandatory in order to get access to production servers. These accesses are limited to a limited subset of Qualifio staff based on a "need to know" and "least access privilege" principles
- User passwords are hashed using SHA-256
- IP addresses available in campaigns statistics are hashed using SHA-256
- 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 CTO, 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	Encryption at rest	Encryption key owner
OVH	France	EU	Participant's PII (structured data) System & access & applicative logs	Y (HDD level) Y (HDD level)	Qualifo Qualifo
AWS	USA	EU	Media files of UGC campaigns System & access & applicative logs Ad-hoc PII extracts	Y (S3 level) Y (applicative) Y (applicative)	AWS Qualifo Qualifo + user's secret
Azure	USA	EU	Backup of participants PII (DB)	Y (applicative)	Qualifo
Google	USA	EU	Ad-hoc PII extracts requested to support	Y (applicative)	Qualifo + shared secret

Encryption of data in transit

From To	OVH	AWS	Azure	CDN77
OVH		TLS	TLS	TLS
AWS	TLS		TLS	TLS
Azure	TLS	TLS		N/A
CDN77	TLS	TLS	N/A	

Physical and Environmental Security

Thanks to the asset inventory maintained by Qualifio, the location of each mission critical information and IT assets is known. A policy is rolling out in order to ensure that these assets are located in a data processing facility compliant with ISO27001 and/or SOC2 standards.

Data processing facilities

Our core-business applications are located inside datacenters of the OVH group, 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
- ...

Our current footprint in terms of geographical spread is 1.400 km across Europe.

More information about the physical & environmental security can be found under the sub-processors section.

Qualifio's Offices

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

Qualifio's laptops

Qualifio laptops are governed by a Laptop policy that enforce technical and operational measures to protect the device and its content. Laptops are verified periodically for their conformity with the policy.

The policy defines, amongst other measures:

Hard drive encryption

In order to prevent data leakage due to theft of a Qualifio's laptop, data encryption of hard drives is enforced. The full list of encrypting keys is kept by Qualifio, the hard drive being crypt-erased (by deleting the encryption key), once an employee leaves the company.

Antimalware protection

Qualifio laptops are protected by an antimalware protection that is always active. This antimalware protection is managed at the company level for all Qualifio laptops.

Software updates

Laptop 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.

In case the device is left at the office outside business hours, it must be placed in a locked cabinet.

USB Mobile Storage Device

It's strictly forbidden to use any USB mobile storage device on any asset of the organisation. Please refer to the data classification policy for the allowed platform to store or share (internally or externally) Qualifio's data.

Operations Security

Backup Policy

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

- Databases
- User provided content hosted by Qualifio
- Documentation
- Internal Files
- Emails
- Application code

Backup of databases

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

For this reason, all databases containing PII data are:

- Replicated:
 - Data records are replicated in real time on at least two database nodes, located in distinct datacenters.
 - The replication is ensured via an encrypted channel.
- Backed up:
 - All databases backups are encrypted
 - The storage is performed on any of Qualifio EU datacenter
 - Retention period is 180 days.
- Testing of backups:
 - Backups are tested for integrity. Because we use multiple database technologies according to the type of data that must be stored, the testing of backups is performed on databases using a "round robin" scheduling over the different exercises.
- Frequency of backups:
 - Backups are performed on the multiple database technologies in order to comply with our defined RPO (Recovery Point Objective) and RTO (Recovery Time Objective).

Backup of User Provided Content hosted by Qualifio

Content provided by our customers is stored between multiple Qualifio EU data centers (object based storage). Content is versioned and replicated in order to meet our RTO/RPO.

Documentation & internal files

Documentation and internal files are hosted on Google Drive (Data region enabled is Europe). Backup of this data is ensured by Google, as part of the data region policy (<https://support.google.com/a/answer/9223653>).

Emails

Our emails are hosted by Google Mail (EU servers), 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

The complete Qualifio's application infrastructure is protected against DDoS (Distributed Denial-Of-Service) by the OVH Anti DDOS infrastructure. After this line of defence, our infrastructure is protected by network equipment performing load-balancing and traffic throttling / rate limiting, as well as a firewall to deny access to non-public services and protect from common attacks.

Logging & Monitoring

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

All logs (application and system) are already shipped and aggregated inside an Elasticsearch cluster. The following platform are used to support our logging, monitoring and alerting needs:

- Monit: reactive monitoring + alerting and implementing safeguard or emergency measures to win precious minutes when something happens.
- ELK Stack: Logs aggregation to centralise all events on the platform.
- Uptime & FreshPing : External monitoring of our services
- Prometheus with Alert manager
- External port scanner to detect change of surface attack of the infrastructure

Remote access control & Intrusion Detection & Prevention

All our servers are protected against intrusions by exclusive access through a management VPN, in conjunction with a protection against brute force attacks. SSH access is always based on private-key authentication.

Services exposed to the internet only do so via the HTTP protocol and are protected by a Level 7 Filtering HTTP-proxy.

IDS is implemented through the use of Unix audit events gathered and centralised on a separate server from the one under surveillance.

Communications security

HTTPS and SSL

Front-end: All customer's domains are only available through HTTPS.

Back-office is also exclusively accessed through the HTTPS protocol. At any time, the current certificate status can be checked here:

Engage: <https://www.ssllabs.com/ssltest/analyze.html?d=manager.qualifio.com&latest>

Loyalty: <https://www.ssllabs.com/ssltest/analyze.html?d=manager.loyalty.qualifioapp.com&latest>

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

The cipher suite used is `EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH`

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
- Bug: A correction to an existing feature of the product. Bugs also include incidents.
- Customer project: A specific request for one customer such as custom integration.

Features

All features are defined using "User Stories" created together with the Product owner, a representative of the development and QA teams.

Features are analysed from a security and privacy perspective in order to ensure Privacy and Security by design and by default.

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

In order to ensure the quality of developments, Qualifio uses strict definitions to define that a User Story is "Ready" (ready to develop) and "Done".

Bugs

All bugs are evaluated by the Product team and, based on their criticality, are scheduled in a future Sprint or retrofitted in the current sprint.

Customer projects

All customer projects are handled by Project Managers that make the link between the customer and the internal development process. User stories for customer projects are defined and are scheduled into the future sprints.

Teams

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

- Product team (PT)
- Quality Assurance team (QA)
- Agile Development team (Dev)
- Integration team (Int)
- Infrastructure team (IT)

Development practices

Qualifio maintains and operates a single codebase for all its clients. This code is developed with a strong focus on quality and performance. To achieve these goals, different techniques and coding standards are used such as:

- Pair programming
- Test Driven Development
- Code reviews

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

- Using continuous integration and deployment for small, incremental steps
- Using framework and components whenever it's possible (mainly on new applications)
- Evolving existing applications instead of re-starting from scratch

Separation of environments

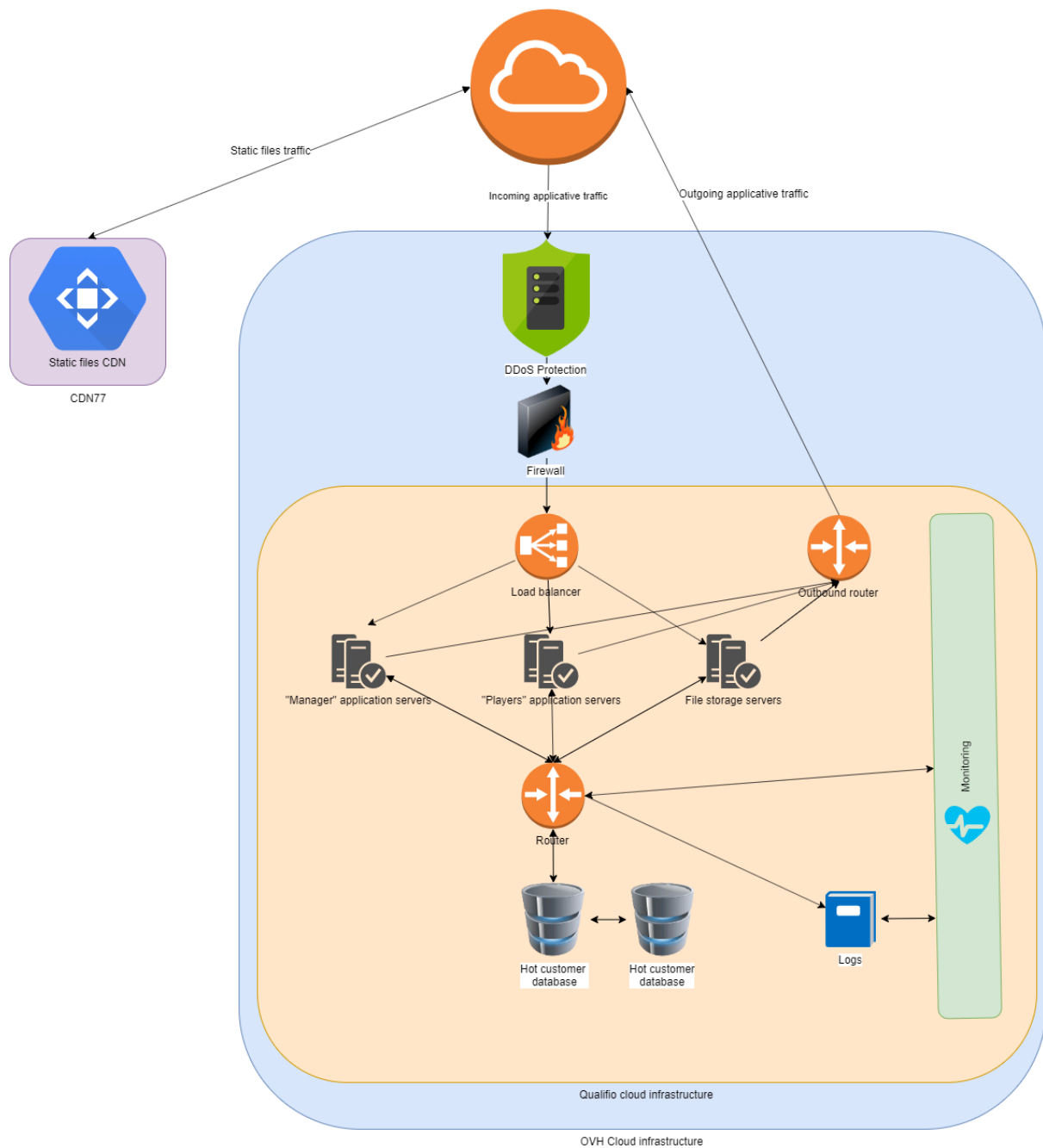
Environments are separated and only production servers contain real “personally identifiable information” (PII), developers and testers are working on dummy test data in the respective environment (development, Q&A).

Environments accesses

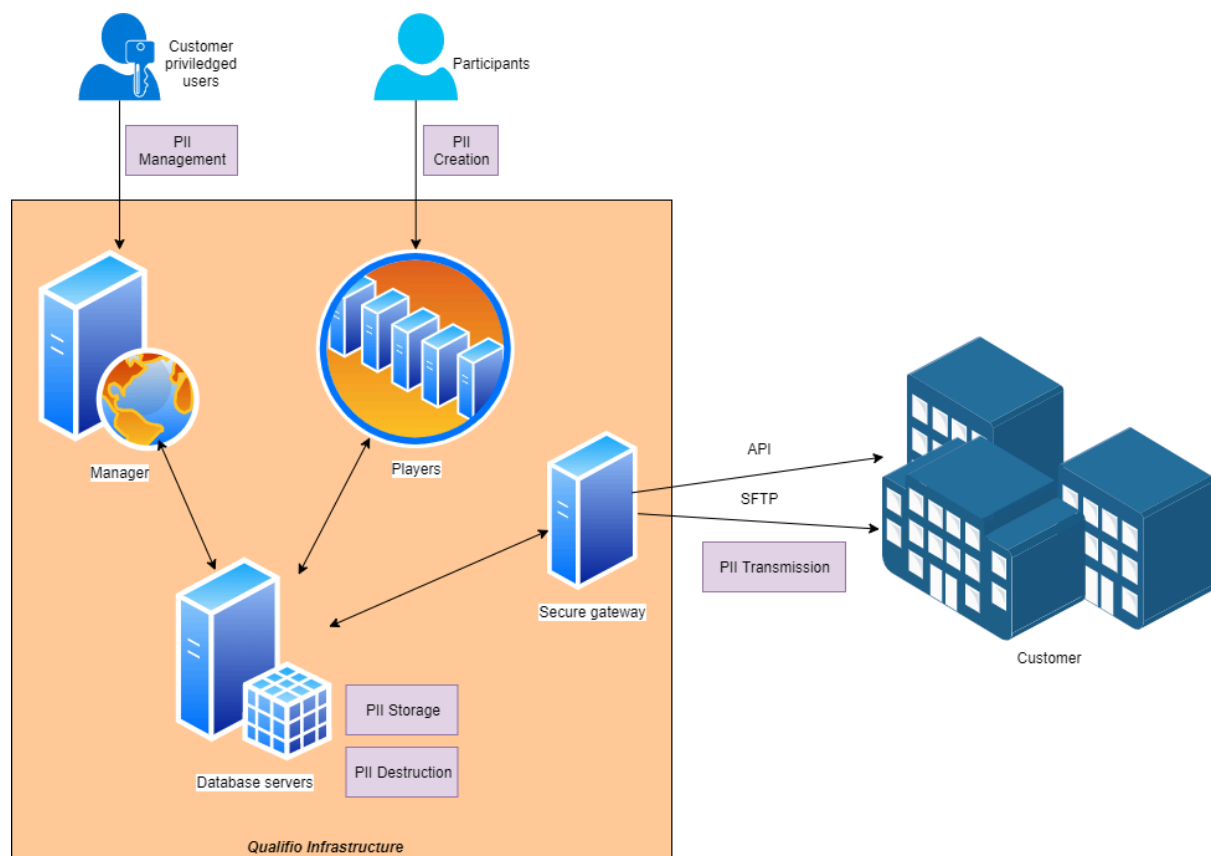
Qualifio has different environments, for development, QA, acceptance and production. Database access is restricted per user on an **assigned role** basis, and per application on a **scope** basis. Access to the production database is limited to a very limited pool of users.

The IT security team is responsible for assigning a role, per environment, to each member of the IT team.

High level architecture



Data flow & PII lifecycle



Code review & Testing

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

All Qualifio's components have been developed internally and are updated by our IT team located in Louvain-La-Neuve (Belgium).

Peer Code Review

All code ready for production is countersigned by 1 to 3 other internal developers based on the project.

Testing

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

Qualifio uses a mix of:

- Unit tests: automated, application-level
- Integration tests
- End-to-end tests
- Manual regression testing
- Pre-production End user simulation

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

These tests are automatically triggered by our continuous delivery platform.

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, i.e reducing the number of Releases with unexpected outcomes or requiring roll-back.
- 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 projects, bundled changes to an existing service (releases containing multiple enhancements/fixes) and critical changes to an existing service must go through the Release Management process with appropriate approvals (Head of Product or Product Team / Customer Project Team, DPO and CISO).
- Whenever possible, changes to an existing service should be bundled together and released on a regular (weekly) basis using the Release Management process.
- A single "Release Manager" must be identified for every Release. The Release Manager will be responsible for successful coordination and execution of the Release, as well as ensuring all required documentation related to the Release exists.
- Each Release should be well tested and verified prior to implementation by our QA team.
- All implementation work on the Release should be completed by the Planned End Date/Time.
- Validation that the Release has been completed successfully should be confirmed through post-release testing.

Release Workflow

- Release Maintenance is scheduled on the status page: <http://qualifo.status.io/>.
- All features/tickets are available in pre-production environments.
- All features/tickets are reviewed by QA on pre-production environments.
- All features/tickets are updated with the correct label: Production Ready.
- Release Maintenance is flagged as started on the status page.
- Preproduction environments are merged into production environments.
- Release is correctly tagged.
- Release Note link is added to GitLab tag
- Release Note is fully completed (correct expected/spend time, presences, all tests green).
- Release Maintenance is closed on the status page.
- Release Communication (internal and external).

Lesson Learned

Each Release must have a post analysis on problems we encountered. These information will be attached to the Release Note:

- Description
- Severity
- Impacts
- Solutions to observe for next releases
- Details

Production Data

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

Information Incident Management

Incident Management Procedure

Qualifio has implemented an Incident Management Procedure. It handles appropriate duties for responding to, mitigating and to remedying Security and Privacy incidents. The policy is available on-request.

Customer Support

Status Page

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

Online assistance

All Qualifio's users can contact the Helpdesk in-app or via : <https://www.support.qualifio.com>

Technical vulnerabilities management and Patching policy

Technical vulnerabilities patching

Technical vulnerabilities patching is prioritised based on the "Common Vulnerability Scoring System"(CVSS) as follows:

	Critical	High	Medium	Low
Patching delay as from notification	48 hours	48 hours	15 business days	60 business days

Other patches and updates

Patches are handled during the quarterly maintenance week included in the team's roadmap.

Time frame: 3 months

How: maintenance task in the next maintenance week

Major version changes

Major version changes have to be planned and handled through a project included in the team's roadmap.

Time frame: 6 months

How: detailed project included in the roadmap

Fair use policy

- Qualifio is not a “second screen” platform for broadcasters. More details are available in our FAQ :
<https://qualifio.zendesk.com/hc/en-us/articles/360017574173-How-many-concurrent-users-can-be-connected-at-the-same-time-on-Qualifio-campaigns->
- The Qualifio systems work as a distributed application, the system uses a load balancer to steer participants to a computing node : the "Player Server". This node is able to withstand around 30.000 active sessions (accessed in the last 20 minutes). Campaign's type & settings have an impact on concurrent sessions.
- The memory usage of the VMware cluster is targeted at a 75% usage, leaving room for peak activity.
- The system works on a baseline of 30 active nodes. If needed, additional units can be deployed in about 20 minutes; or deployed for a special forecasted peak operation on dedicated resources.
- Additional physical resources may be injected into the VMware system in 1 hour if needed.
- The basic resources are shared across all customers and participants, requests will be sent to the least active server based on recent activity history
- Please get in contact with Qualifio Helpdesk if you think your campaign will reach more than 10.000 concurrent users.
- It is possible to add additional virtual machines to a specific account & guarantee a unique access to resources.

Business Continuity & Disaster Recovery

Redundancy

In order to ensure its high SLAs, Qualifio makes use of 5 data centers , all ISO27001 and SOC2 Type II certified.

. This setup ensures a geographical spread of 1.400 km across Europe.

Business Continuity

Qualifio has defined business continuity scenarios that respond to disruptions due to Environmental, Technical or People factors.

Those scenarios have been defined to meet the RTO and RPO approved by the Management.

RTO

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

All backup solutions deployed in Qualifio should ensure a RTO of maximum 24h, when they protect Qualifio's customer data. When the protected data is Qualifio's internal data, this RTO should not exceed 48h.

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 application and the type of information

	Campaigns	Rewards Programs
Customer data (excluding UGC)	15 m	12h
Customer UGC	15 m	N/A
Configuration	24h	24h

For all data not covered by the table above and in particular for all internal data, a RPO of 24h is applicable.

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

Disaster Recovery

A disaster recovery procedure has been defined by the CTO to recover the production systems in case of disaster (recovering from scratch). The disaster recovery applies for all production systems needed to provide the Qualifio service to our customers. This disaster recovery procedure is reviewed yearly.

Compliance

Security Audits & Reports

Qualifio is running periodic assessments on the security of the product. They can be performed by a 3rd party (external audit) or internally (internal audit).

External audits

Penetration test

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

Qualifio is contracting with external parties to conduct penetration tests missions 2 times a year.

The latest pen test was conducted in *[Data_Latest_Pen_Test]*. A declassified version of the pen test report is available upon request for our active customers by contacting security@qualifio.com.

Customers on-demand Audits

Qualifio works with more than 300 enterprise organisations across Europe in various sectors (media, banking, retail, FMCG, etc.). Each of our clients has high security and data protection standards. This is why Qualifio is willing to share the results of audits (with them in order to guarantee the existence, monitoring and continuous improvement of its management systems related to the Information Security (ISMS) and PII (PIMS); by external auditors.

This mechanism has been put in place in order to prove our compliance with international standards and facilitate security assessments from customers, which is time-consuming on both sides.

Similar to most SaaS companies in our yearly licence price range, we do not allow our customers to organise their own audits of Qualifio, as those exercises are highly time-consuming for our teams. As a fast-growing company it does not scale to follow up different custom audits.

Additional on-demand security audits requests (security assessment and penetration tests) or requirements can be analysed by our CISO for Platinum customers only. Please refer to our General Terms & Conditions & take contact with your account manager if you have any questions related to on-demand audits.

Internal audits

At the same time, Qualifio is running audits internally. These audits include:

Vulnerability scan

Qualifio is constantly scanning its infrastructure against open ports or well known vulnerabilities.

Docker images are signed and scanned for vulnerabilities before being deployed.

Static Code Analyzer

- Sonarqube is used as Static code analyser

Insurances

Qualifio's activities are covered by the following insurances:

- Professional Indemnity Cover and Public Liability Cover
- Cybersecurity cover

NIS2

Qualifio has been registered as a NIS2 "Important Entity" under the Belgian CyberSecurity Authority with ID 0822741924.

Why aren't we ISO 27001 or ISO 27701 certified?

We've implemented an Information Security Management System (ISMS) and a Private Information Management System (PIMS) respectively based on ISO27001 and ISO27701 standards.

Those Management Systems are regularly reviewed and improved. This document, based on the structure of the ISO controls is a proof of our commitment and adherence to those ISO Standards.

We also make sure that our suppliers are as secure as us. Indeed, our supplier security policy requires that all our sub-processors, that are processing customer's information, must be ISO2001 certified or provide a SOC2 Type 2 report.

Convinced by the importance of an ISMS and PIMS, the Management is fully supporting the Management Systems and their continuous improvement. However, it is a Management decision to not enter in the ISO27001 certification process, based on the current size of the company and its agility (time to market).

Data protection and privacy

Qualifio as "data processor"

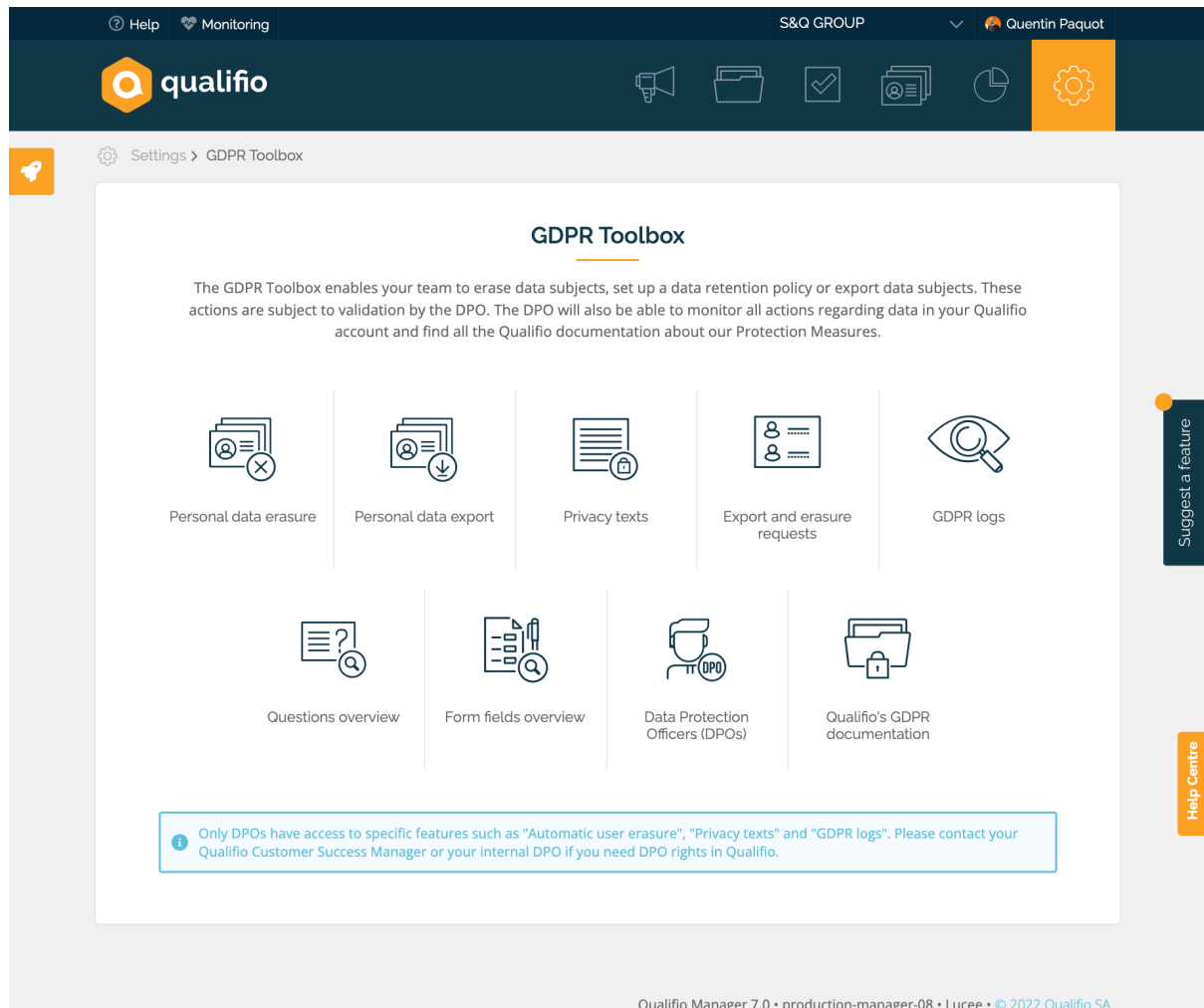
When personal data is asked to a campaign's participant, Qualifio acts as a « data processor », processing data on behalf of its clients (the « data controller »).

Accordingly, Qualifio has no direct relationship with the individuals whose information it receives from its clients. Qualifio does not control such information, does not select or determine the specific types of data it processes, and does not determine the purpose for which it is processed.

Qualifio's Data Privacy management interface for customers: The GDPR Toolbox

Qualifio developed a set of features called the 'GDPR Toolbox' specifically for the DPO & team of its customers. The GDPR Toolbox enables your team to set up a data retention policy and export or erase all data linked to a specific data subject. These actions are subject to validation by the

DPO. The DPO will also be able to monitor all actions regarding data in your Qualifio account and find all the Qualifio documentation about our Protection Measures.



The GDPR Toolbox has 2 different views:

- View for DPOs
- View for users who are not appointed as DPO

The GDPR Toolbox is accessible for Marketers & Admins. Although, as long as they are not DPO they will not be able to validate erasure or exports, view the logs, they'll only see their requests and they won't be able to name other users DPO.

In the Advanced User rights (not in the GDPR Toolbox), you also have 2 possibilities:

- Only let admins access the GDPR Toolbox
- Only let admins do exports overall in Qualifio

PII Retention Policy

All PII's except IP addresses

By default, PII of end-users (participants) is kept for 24 months in the Engage module. This Retention Period can be reduced by users having the "Data Protection Officers (DPO)" role defined within the account settings. (*see Data subjects erasure / Automatic*)

If your DPO sets up a shorter Data Retention Period in the account settings, PII collected in participations is deleted after the defined retention period. This means that the whole participant profile linked to the participation is deleted, whereas the anonymous participation data is kept. In other words, regardless of the retention period defined by your DPO, you have access during 24 months to the anonymous statistics of your campaign and during the retention period set by your DPO, also to the identified data of the participants.

After 24 months, all data linked to participants (PII) and participations (anonymous) are completely deleted from our operational systems. However, your DPO can also configure the full deletion (identified and anonymous data) after the retention period mentioned above.

Please note that deleted data can still reside in its original forms in backups, kept in non-operational systems in a medium that requires specific procedures to be accessed. This, in order to guarantee the business continuity of the application in case of an incident. A period of 6 months is necessary to guarantee a full deletion of this data in our backups.

IP addresses

IP addresses are PII for which specific processing is performed by our systems.

Within the Qualifio application, the customer has different options:

- In the case of 'identified campaigns', IP addresses are hashed (with multiple "salt" information) before being stored into the Qualifio database.
- In the case of an anonymous campaigns, the customer has the choice to:
 - collect and store the hashed version of the IP addresses in the Qualifio database (as for an identified campaign)
 - Not collecting the IP address. In this case, a random string will be generated by our systems and stored into the Qualifio database.

Within the underlying technical infrastructure, Qualifio may keep the IP addresses of the visitors, for a period not exceeding six (6) months, in order to have the necessary traceability to ensure

the security of its information system and its products and services. These access logs allow Qualifio to analyse accesses to its systems and platforms and determine the origin of possible incidents and alerts (fraudulent access, misuse, etc.) by establishing correlations between log data. These access logs are not used for any other purpose than technical and organisational security.

This is a recommended retention period from a security perspective (to have historical data to investigate in case of an incident), and an acceptable delay acknowledged by data protection authorities.

Data subjects erasure

The GDPR toolbox allows :

1. Bulk participant erasure, in case you want to erase personal data (PII) from users within a certain time range;
2. Manuel participant erasure, if you're looking to erase all PII concerning a specific user/profile based on their email, first name and last name.
3. Automatic participant erasure: this feature is only accessible to DPOs and allows to set up automatic deletion rules based on your data retention policy. For instance, you can choose to erase all users who participated in a campaign in the last X weeks or months.

Data subjects export

This module allows you to export all data about a specific user (again, based on their email, first name, last name). This will include all data from Qualifio campaigns and from the CRM.

Any request to export Data Subject with the internal help of Qualifio will be done according to the [Segregation of duty](#) principle using the [Exchange of files with customers](#) procedure.

Default data protection/privacy texts

Within this module, you can set up default privacy texts for all your campaigns based on the website on which they will be published. You can either place this text underneath the identification form, or in a dedicated tab accessible from the top right corner of the campaign. You can also choose to do both.

GDPR requests

As a DPO, this is the place you'll be able to manage all requests from your users. You can accept or refuse the erasure or GDPR export of users data, and keep track of all such requests.

GDPR logs

In the Engage module, as a DPO, GDPR logs help you get an overview of all personal data manipulations in your Qualifio account. For example, you'll be able to see who viewed statistics, checked CRM info, or exported reports. Logs can be sorted by date, action or user. You also get the possibility to export all logs. These logs are kept for 12 months.

Overview of all questions

This module gives you an overview of all questions created in all campaigns of your Qualifio account. Questions are listed from the most recent to the oldest. If you see something suspicious, you may suspend the question immediately and directly from this module. This is particularly useful to monitor whether sensitive data is (inadvertently) being collected within your campaigns.

Overview of all identification fields

In the Engage module, this module gives you an overview of all identification fields created in all forms of your Qualifio account. If you see something suspicious, you may suspend the question immediately and directly from this module. This is particularly useful to monitor whether sensitive data is (inadvertently) being collected within your campaigns.

DPO account management

In the Engage module, this is where you appoint the DPO(s) for your Qualifio account. There are a series of options for the DPO, such as whether they want to review all GDPR exports or whether IP addresses should be collected in anonymous campaigns.

Restitution of Data at the end of the contract

Clients can export and delete Data at all times. At the end of the contract, the accounts & databases of the customer will be deleted.

Qualifio GDPR protection measures documentation

This is where you'll find Qualifio's standard GDPR agreement, along with our other measures for data protection. Those documents will be updated in time to reflect our latest measures.

Access the GDPR Toolbox via API

The whole GDPR Toolbox has been built on an API and is accessible via this API. You can thus erase users, exports data, etc. all from your master database, removing manual action and possibility of mistakes.

Consent management and opt-in

In addition to the GDPR toolbox, the Qualifio software also includes a section for opt-in and consent management. If the legal ground for processing is consent, customers can configure one or more opt-ins with their identification form in order to lawfully process PII .

The main use case is to consent to newsletters subscription (opt-in), however the opt-in manager also includes categories for other use cases, such as contracts, rules or processing by 3rd-parties. The consents collected are available in the statistics for each campaign or globally for the account in the opt-in statistics. Furthermore, in order for the customer to fulfil the obligation for demonstrating valid consent, the statement to which the user consented is versioned.

Organisational measures to ensure security and protection of PII

Data Protection Officers

In order to ensure the independence of the Data Protection Officer, we've appointed an external (DPO) from the company "GDPR Agency" that is reachable through the email dpo@qualifio.com.

We ensure that our Data Protection Officer

- Is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data.
- do not receive any instructions regarding the exercise of those tasks.

- are bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.
- won't be dismissed or penalised by the Controller or the Processor for performing his tasks.
- don't perform any such tasks and duties do not result in a conflict of interests.

Qualifio will support the Data Protection Officers in performing the tasks referred to in Article 39 of the GDPR by providing the resources necessary to carry out those tasks and access to Personal Data and processing operations, and to maintain his or her expert knowledge.

Human resource measures

Confidentiality clause in employment contracts

[See "Confidentiality Clause in Employments Contracts" section](#)

Security awareness and continuous education of staff

[See 'Security awareness and continuous education' section](#)

Data Breaches procedures

Incident intake

Anyone can notify Qualifio of a security and/or data breach through the following email addresses: dpo@qualifio.com and/or security@qualifio.com.

The following information must be provided:

- the nature of the data breach
- categories of data impacted
- number of records
- number of data subjects
- any other information that led you to presume the data breach
- contact details (DPO or any other contact point)

If the information is not sufficient, the person that is investigating the incident will request more information from the person that has reported the breach to Qualifio.

The DPO team and/or the Security team will acknowledge your request then immediately start to investigate your potential data breach case. An incident ticket will be created in the ticketing system of Qualifio.

Assessment of the incident

The DPO and/or Security team will assess the incoming incident. This investigation will classify the incident in the following cases:

- False positive
- Security breach without PII breach
- Security breach with a PII breach

In case of a “false positive”, the incident will be updated in the ticket management system of Qualifio and the incident will be closed.

Incident handling

Handling the “Security” aspect of the incident

The security team will go through the following activities:

- Containment: The impacted systems will need to be isolated from the operational environment in order to avoid the incident to spread to other assets
- Mitigation (optional): The security team will provide a temporary solution in order to fix the issue until a remediation is available
- Remediation: The security team will provide a permanent solution to fix the issue

Handling the “Privacy” aspect of the incident

The DPO team will perform the following activities:

- Assess the breach: The DPO team, with the needed resources will need to assess the breach. This assessment will need to conclude on:
 - The category of data that has been breached
 - The quantity of data that have been breached
 - The impact on the data subject due to the breach
- Notification: As a data processor, Qualifio will inform the data controller without undue delay with the following information:
 - the nature of the data breach
 - categories of data impacted

- number of records
- number of data subjects
- contact details (DPO or contact point) where more information can be obtained
- Measures taken or proposed to be taken to address the personal data breach (including when appropriate, measures to mitigate possible adverse effects)
- Document: Qualifio will also document the data breach detected in a record of personal data breaches.

At any stage of an incident, and whatever its category (security and/or privacy), Qualifio could request the intervention of a digital forensics in order to collect legal evidence of the breach.

Incident closure

After that the incident has been handled, a “post mortem” analysis will be performed and documented. This report will contain:

- The root cause analysis
- A timeline of the incident
- Lessons learned
- Action plan

The CISO will make sure that the incident has been correctly documented in the ticketing system. In case of a PII data breach, the DPO will make sure that the incident has been correctly documented in the personal data breach register.

Transfer of PII to the customer

Automatically push of PII to customer's information system

Qualifio is able to push data collected in different ways:

- Real Time Push (REST over HTTPS)
- FTPS Push/Export
- Amazon S3 Bucket Export

Please find more information in this FAQ :

<https://qualifio.zendesk.com/hc/en-us/articles/360019072914-Push-export-data-to-your-CRM-Marketing-Automation-Platforms-other-MarTech-software>

Manual transfer of PII to customer

Transfer of data exports outside Qualifio is only allowed through a strict procedure to ensure that the correct file has been received by the correct recipient. Based on the data classification of the content of the file, one or more of the controls will be activated:

- Send a temporary link to the file to the recipient email address
- Limit the number of download of the file
- Encryption of the file and send the encryption key through a second secure channel

All accesses (export and consultation) of customer data by the Qualifio staff are logged in the GDPR Toolbox.

Technical measures to ensure security and protection of PII

Privacy by design and by default

We are also implementing a policy of 'Data Protection by Design and Default' to ensure we are systematically considering the potential impact that every project or initiative might have on the privacy of individuals. This is especially sensitive with the Product people at Qualifio (designing new features) and, of course, the IT team.

Cookie Management

Cookies and their usage are described in our "Cookie Policy", which is available upon request to dpo@qualifio.com.

Deletion of PII

When a deletion request is triggered from the GDPR Toolbox, the related PII are anonymized in order to keep them in an aggregated form in the statistical module.

This anonymization of PII is propagated to all database instances. The PII residing into our archives will be destroyed after the retention period of the backup.

All hardware containing PII that needs to be decommissioned will follow a secure deletion procedure of all its hard drives (using hdparm secure deletion tool) before being removed from our infrastructure.

Restricted access to production Personal Data

[See "Production Data" section](#)

Physical access to our offices

[See "Physical and Environmental Security" section](#)

Computers

[See Qualifio's laptop section](#)

IT security controls

Please refer to sections:

- [Asset management](#)
- [Access control](#)
- [Cryptography](#)
- [Physical and Environmental Security](#)
- [Operations Security](#)
- [Communications security](#)
- [Information Systems Acquisition Development and Maintenance](#)
- [Information Incident Management](#)
- [Business Continuity & Disaster Recovery](#)
- [Compliance](#)

Contractual agreements with Customers

As part of our contractual agreements with customers, the following GDPR related documents will be issued:

Data Processing Agreements

Clear contractual agreements with clients according with article 28, namely impeding Qualifio to disclose, exploit or resell any personal data to third parties ;

Records of Processing activities

In accordance with article 30 (2) of the Regulation, our record of Processing activities includes:

- Our contact details, together with those of the Data Controller on whose behalf you are acting and, where applicable, of the Processor's representative and the Data Protection Officer.
- The categories of processing carried out on behalf of the Data Controllers.
- Where applicable, any transfers of the Data to a third-party country together with documentation showing the existence of appropriate guarantees for each transfer.
- A general description of Technical and Organisational security Measures.

Qualifio's sub-processors

Clear contractual agreements with sub-processors, according with article 28, namely ensure that our Processors provide sufficient guarantees to implement appropriate Technical and Organisational Measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.

Qualifio takes adequate safeguards when transferring personal data out of the European Economic Area (EEA) or outside any country for which an adequacy decision has been made. Standard Contractual Clauses from the European Commission (or other guarantees provided for in art 46 of the GDPR) are contractualized. Next to this, Qualifio assesses (Transfer Impact Assessment TIA) if there is anything in the law or practice of the destination country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools and identifies and adopts supplementary measures when needed (encryption with key management by Qualifio, pseudonymisation, split processing, ...).

Where that other Processor fails to fulfil its Data protection obligations, we shall remain fully liable for the performance of that other Processor's obligations.

Qualifio works with sub-processors to carry out processing activities necessary for the provision of services to the Customer. A list of those sub-processors and related processing activities is located on the Qualifio sub-processors page available from the GDPR Toolbox or at this URL: <https://gdpr.qualifioapp.com/subprocessors>.

Artificial intelligence and Compliance

Qualifio has introduced internally developed AI features to enhance content generation within user campaigns. These features utilize the OpenAI API for generating content efficiently and effectively. Below is a detailed and enriched explanation of how these AI capabilities function:

Key Features of Qualifio's AI Integration

1. Content Generation Powered by OpenAI:
 - Qualifio's AI tools leverage OpenAI's advanced language models to generate high-quality content for campaigns, such as quizzes, questionnaires, and more.
 - Users can input specific prompts or commands, and the AI generates tailored content in seconds, streamlining the campaign creation process.
2. User Input-Driven Data:
 - The data sent to the AI model consists solely of user-provided inputs (e.g., prompts or commands). Qualifio ensures no personally identifiable information (PII) is shared with OpenAI, maintaining user privacy and compliance with data protection regulations.
3. No Data Used for Training:
 - Data shared with the OpenAI API is not utilized for training or fine-tuning the AI models, guaranteeing that user inputs remain confidential and are not stored for model improvement.
4. Control over Content Generation:
 - The AI features are enabled by default. However, they can be deactivated upon request to avoid the AI model to generate content, ensuring full control over when and how these tools are employed.

Benefits for Users

- Efficiency: The AI question generator can produce complete questionnaires in seconds, significantly reducing the time required for campaign preparation.
- Customization: Generated content is fully editable, allowing users to refine questions and answers as needed before finalizing their campaigns.

- Compliance: With strict adherence to GDPR guidelines, Qualifio ensures data privacy and security throughout the process.

Use Cases

- Ideal for creating quizzes, polls, and other interactive formats that engage audiences while collecting valuable insights.
- Particularly beneficial for marketing teams that frequently require fresh content but have limited time or resources.

In summary, Qualifio's integration of AI-powered tools marks a significant step forward in simplifying and accelerating campaign creation while maintaining a strong commitment to data privacy and user control.

Specific requirements for the Italian market

Introduction

Italy has specific regulations governing contests with prize offerings. To comply with these requirements, Qualifio has implemented a dedicated infrastructure designed to meet Italian legal standards. This is in addition to its primary hosting infrastructure in France, Germany, and Poland.

This document outlines the technical architecture and data flow of Qualifio's solution dedicated to the Italian market. However, it is important to emphasize that ensuring compliance with specific local regulations and individual requirements remains the sole responsibility of the customer.

Infrastructure

Qualifio has chosen Microsoft Azure to host its Italian-specific infrastructure. The datacenter is located in Milan.

Remark: Under contractual terms, Qualifio retains the right to select the most suitable hosting provider and may change this provider at its discretion in accordance with the rules of sub-processor change.

The following components are hosted in Italy:

1. Site-to-Site VPN:
 - A secure, encrypted connection links the Italian datacenter to Qualifio's primary infrastructure.
2. Dedicated Database:
 - Stores all participant data collected during campaigns.
 - Stores configuration and parameters influencing winner selection.
3. Back-End Services for Winner Selection:
 - Components responsible for selecting winners are hosted locally.

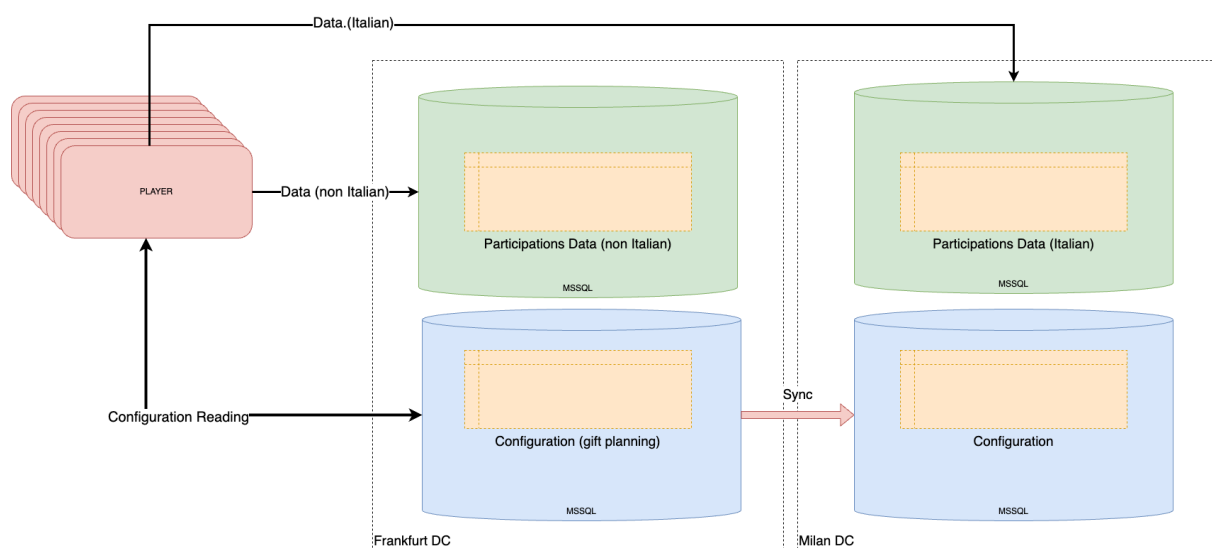
Remark: This configuration does not require hosting the entire Qualifo application or datasets in Italy, only the specific components necessary for compliance.

Architecture

Database hosting

The diagram below shows the configuration of databases:

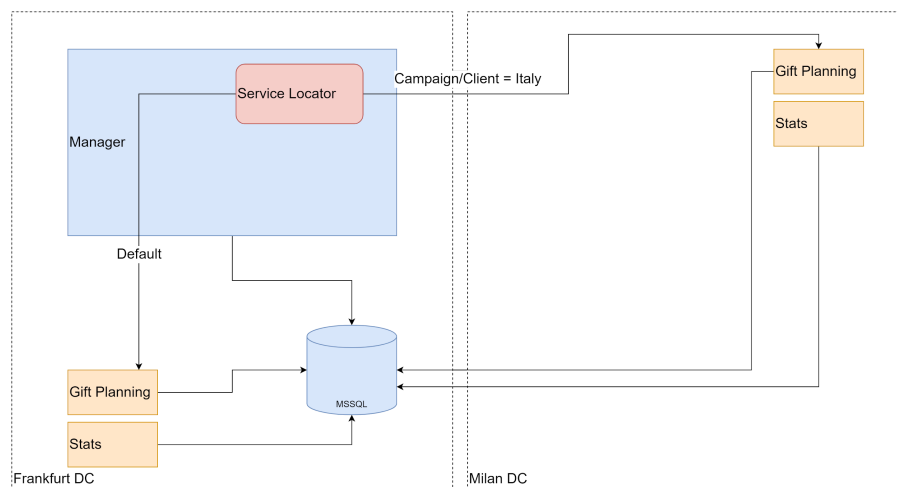
- A Microsoft SQL database instance is deployed in the Milan Data Center with the following structure:
 - All participants data collected during the participation (primary copy of the data)
 - A replication of all configuration elements required to execute / justify the selection of a particular winner (secondary copy). This replication is “near real-time” with respect to creation / update of data.
- In this configuration, services (APIs, processing nodes) are always accessing (reading/writing) the primary datastore
 - In the case of an Italian campaign, configuration is read from the Frankfurt DB, while data is stored in the Milan DB.



Drawing of winners

The general architecture of the solution is depicted below:

- A service locator component will be in charge of deciding how to call the Gift Planning & Statistic component depending on the customer account (Italian based or not)
- These processes will access the central database which is hosted in EU



Account setup and limitations:

(1) As the rules to select the location of data are based on the client account, it is required that a dedicated account be used for all campaigns subject to Italian regulation. It is not desirable that all participations are treated on the Italian specific setup.

(2) The configuration data, in particular the gift planning for Instant-win campaigns, are mirrored in a primary-secondary configuration which means that mirrored data will not:

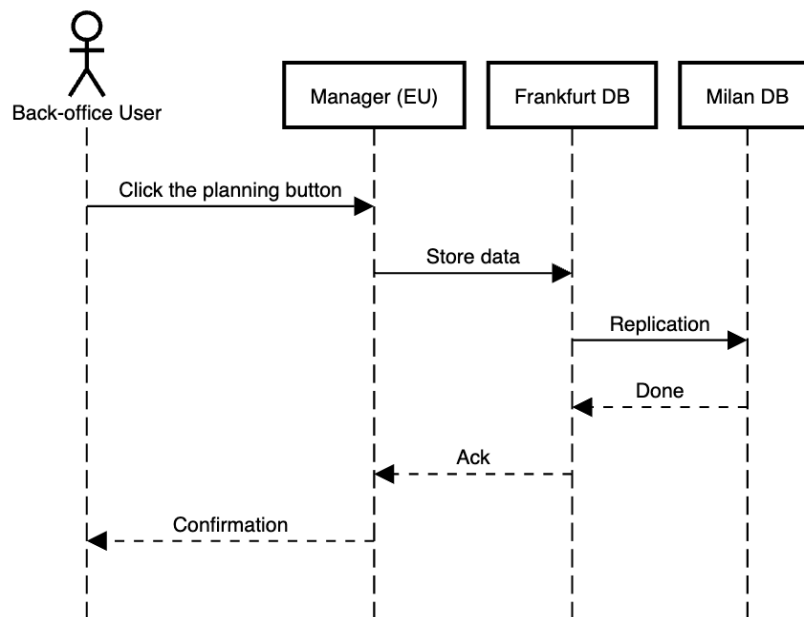
- Be used when performing back-office actions
- Be synchronised back with the master database should any local change happen (which will not happen because no process will be allowed to access this database)

(3) The synchronisation will be "near-real time" meaning there might be a (usually small) delay between an update on the master and the corresponding update on the secondary node.

Data flow

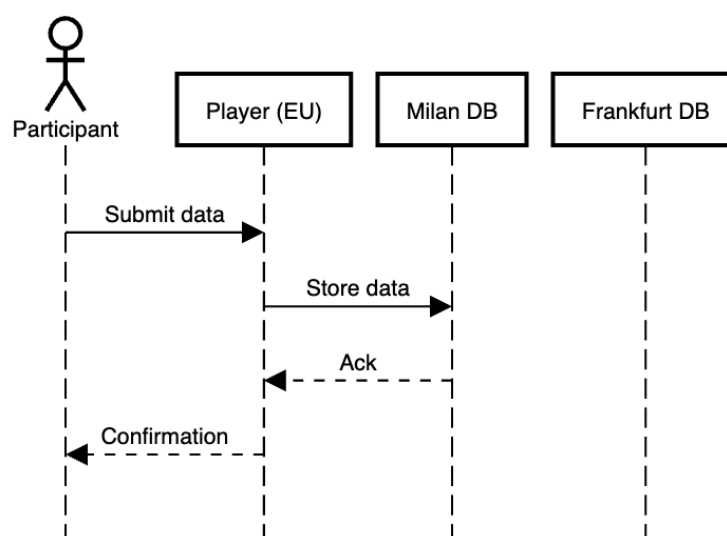
Configuration of gifts (before campaign start)

Configuration of gift planning

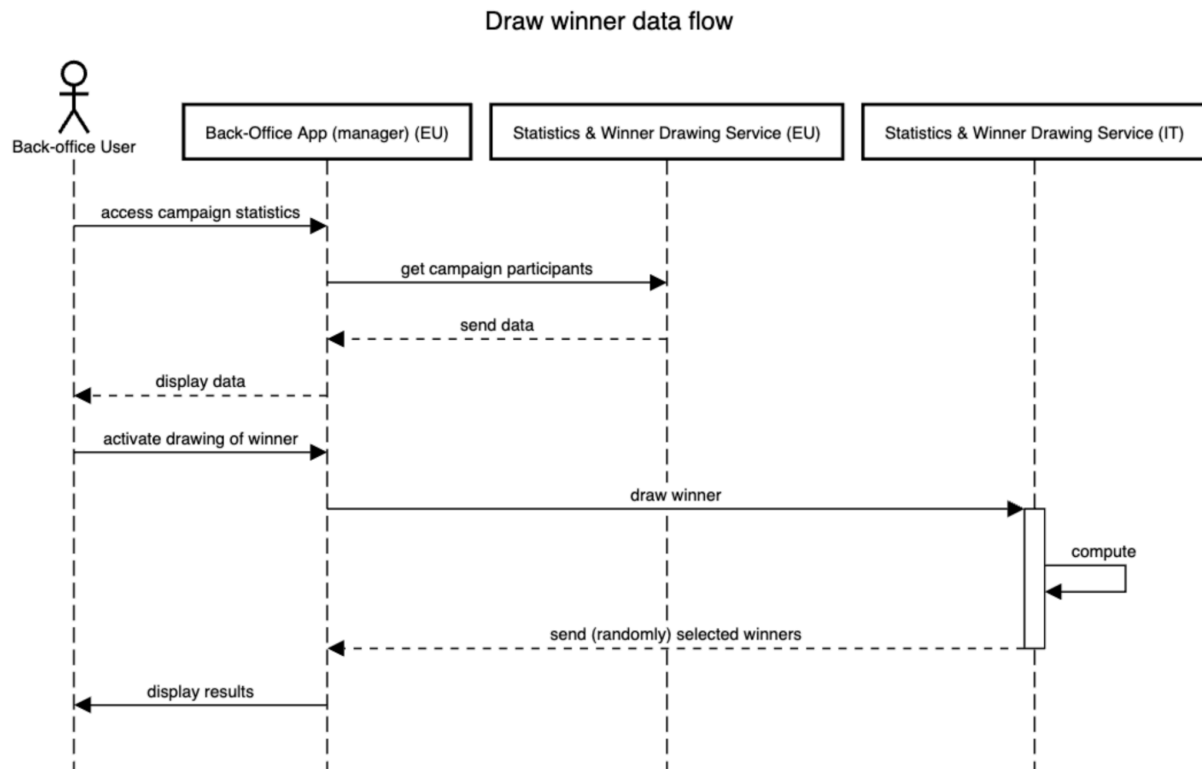


Participation (data collection phase)

Participation / Data collection



Drawing of winner



Annex 1: Definitions

- “Data Breach” means a Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal data transmitted, stored or otherwise processed;
- “Data Controller” means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- “Data Processor” means a natural or legal person, which processes Personal data on behalf of the Controller;
- “Data Protection Officer” (“DPO”) means a person who is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements;
- “Data Subject” means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- “Organisational Measures” mean the measures relate to the system's environment and particularly to the people using it.
- “Personal Data” means any information relating to an identified or identifiable natural person (“Data Subject”);
- “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- “Supervisory Authority” means an independent public authority which is established by a Member State pursuant to Article 51;
- “Technical Measures” mean the measures that directly involve the IT system.