Qont PRI Cloud

Overview

Qont PRI Cloud delivers Portable Risk Intelligence as a service.

It provides direct access to Qont's core risk-analysis systems through secure APIs built for businesses, developers, and enterprise clients.

Every connection runs through Qont's private infrastructure designed to process, evaluate, and return structured risk data — anywhere, at any time.

How It Works

Qont PRI Cloud connects external systems to the same core technology used inside Qont's own products.

Requests pass through a controlled environment where they are authenticated, processed, and returned as structured intelligence.

Clients receive immediate risk outputs that can be embedded into dashboards, software, or enterprise decision tools.

Architecture

The cloud operates globally with dedicated regional servers and support hubs where available.

All systems are managed directly by Qont and maintained under a single operational standard.

Routing adjusts dynamically based on performance and availability.

Each region aligns to Swiss oversight and governance requirements.

Integration

APIs and developer tools make PRI Cloud accessible for risk modeling, operational systems, and analytical workflows.

Activation requires approval and licensing.

Once approved, clients receive secure keys and documentation for integration.

Use is always controlled under Qont's Terms, Privacy Policy, and Data Processing Agreement.

Security

Qont maintains best-effort protection for all active environments.

Traffic is authenticated, logged, and monitored for abnormal behavior.

Encryption is applied wherever possible, and access to systems is tightly controlled.

Data is processed only for legitimate operation or lawful reasons.

Reliability

PRI Cloud is built for resilience with monitored uptime, controlled maintenance, and a recovery framework that protects critical infrastructure.

Best-effort backups maintain service integrity, and regional redundancy supports continuity across major markets.

For Businesses

Enterprises can embed PRI Cloud directly into existing systems to measure, report, or automate risk.

Each connection is isolated, auditable, and licensed under commercial terms.

Dedicated support is available for verified clients.

For Developers

Developers can access structured documentation and examples for integration.

Each API is versioned and tested for stability.

Usage limits and authentication are managed through Qont's developer portal.

For Partners

Approved partners may use the official "Powered by Qont PRI Cloud" mark in alignment with branding guidelines.

Co-marketing opportunities and joint case studies are available with review and written approval.

Ethics and Use

PRI Cloud may only be used for lawful, responsible, and transparent purposes.

It cannot be used to exploit, mislead, or harm individuals or systems.

All users are bound by Qont's Acceptable Use and Export Compliance policies.

Terms of Service

Owned and Operated by Qont

Effective Date: 28/10/2025

Applies to: All clients, developers, and organizations accessing Qont PRI Cloud APIs

1) Overview

These Terms of Service (“Terms”) govern access to and use of the Qont PRI Cloud, a professional risk-intelligence infrastructure owned and operated by Qont.

Qont PRI Cloud provides access to Portable Risk Intelligence (PRI) technology for approved clients, including businesses, enterprises, and developers.

By accessing or using Qont PRI Cloud, you agree to these Terms and any applicable addendums, contracts, or data agreements executed between your organization and Qont.

2) Eligibility and Access

Use of Qont PRI Cloud is restricted to approved clients, businesses, and organizations.

All access requires manual review and authorization by Qont.

Qont PRI Cloud does not provide free trials. All usage operates under paid plans or signed contracts.

Access credentials and API keys are assigned individually or per organization and are non-transferable.

Qont may revoke, suspend, or terminate access at any time for misuse, breach, or legal non-compliance.

3) Ownership and Licensing

All PRI frameworks, data models, logic structures, algorithms, and derived outputs are exclusive intellectual property of Qont.

Clients receive a limited, non-exclusive, non-transferable license to use the Qont PRI Cloud API strictly for internal business purposes.

No ownership rights or proprietary interests are transferred through use.

You may not reproduce, replicate, reverse-engineer, or develop competing products or frameworks based on Qont PRI technology.

4) Data Processing and Confidentiality

Qont PRI Cloud may temporarily process submitted data for operational, diagnostic, or compliance purposes.

All client data is deleted automatically after processing or upon contract termination, unless retention is legally required.

Clients must protect all data exchanged with Qont PRI Cloud and ensure confidentiality at all times.

No processed data, system information, or results may be redistributed, publicly displayed, or shared with third parties without written permission.

Reverse engineering, scraping, or extraction of internal logic is strictly prohibited.

5) Use and Restrictions

You may not:

1. Share, resell, or sublicense Qont PRI Cloud access.
2. Circumvent access controls or attempt to discover source systems.
3. Use Qont PRI Cloud for unlawful, discriminatory, or unethical risk profiling.
4. Integrate Qont data into competing PRI services or products.
5. Tamper with API requests, encryption, or data channels.
6. All usage is logged for compliance and audit purposes.

6) Data Retention and Deletion

Data transmitted to Qont PRI Cloud is processed securely and stored temporarily.

Qont deletes customer data after processing or within contractually agreed retention periods.

Upon termination, all identifiable data is removed from active systems unless retention is required by law, audit, or investigation.

7) Billing and Pricing

All access is subject to Qont approval and formal billing.

Pricing, usage limits, and service tiers are defined per contract or invoice.

Continued use after any notice of updated pricing or limits constitutes acceptance of the revised terms.

Non-payment may result in immediate suspension of access.

8) Service and Availability

Qont PRI Cloud is provided “as is.”

Qont makes no guarantees of uptime, uninterrupted access, or compatibility with third-party systems.

Qont may modify, suspend, or discontinue any part of the service or API at any time, with reasonable notice to active clients.

9) Liability and Warranties

Qont PRI Cloud is an informational and analytical infrastructure designed to support decision-making, not replace professional judgment.

Qont provides no warranties, express or implied.

To the fullest extent permitted by law, Qont is not liable for loss of revenue, business interruption, data loss, or any indirect or consequential damages arising from use or inability to use the service.

10) Compliance and Export Controls

All clients must comply with applicable laws, export controls, and international sanctions.

Qont PRI Cloud may not be used, sold, or accessed from restricted regions, sanctioned countries, or for unlawful purposes.

Clients must ensure all usage aligns with global compliance and Qont’s internal security standards.

11) Conflict of Interest and Competition

Qont may provide PRI Cloud access to multiple organizations, including industry competitors, under neutral and non-exclusive license conditions.

No client receives exclusivity or preferential rights.

Use of Qont PRI Cloud does not imply partnership, endorsement, or affiliation beyond the agreed license.

12) Audits and Verification

Qont reserves the right to review, inspect, or audit API usage and data-handling procedures to confirm compliance.

Clients must cooperate fully with any review and provide relevant records or explanations on request.

13) Public Communications and Branding

Clients may not use Qont’s name, logos, trademarks, or product identities in any marketing, materials, or public communications without written approval from Qont.

Any reference to Qont PRI Cloud in external documentation must maintain factual accuracy and proper attribution.

14) Modifications and Updates

Qont may modify the PRI Cloud infrastructure, APIs, pricing, or documentation at any time.

Notice will be provided to active clients when material changes occur.

Continued use after an update indicates acceptance of the revised terms.

15) Termination and Suspension

Qont may suspend or permanently revoke access immediately, without refund, for:

1. Breach of these Terms or contract terms.
2. Security, compliance, or reputational risks.
3. Fraudulent or unethical activity.
4. Termination does not release clients from outstanding payments or legal obligations.

16) Governing Structure and Priority

These Terms serve as the master agreement for all Qont PRI Cloud users.

If a client holds a signed enterprise contract or addendum, that document will override conflicting sections of these Terms.

17) Legal Notices and Jurisdiction

All legal notices or disputes must be submitted in writing to legal@qont.net.

Dispute resolution, arbitration, or court proceedings will follow the governing law and jurisdiction defined in each client's executed contract.

18) Entire Agreement

These Terms, together with any signed contract or policy addendum, form the complete agreement governing Qont PRI Cloud use.

No verbal agreements or external representations override these Terms.

Privacy Policy

1) Overview

This Privacy Policy explains how Qont collects, processes, and protects data handled through the Qont PRI Cloud platform and its associated APIs.

It applies to all clients, developers, organizations, and any individual whose data may be processed through PRI Cloud systems.

By using Qont PRI Cloud, you agree to this policy.

Qont provides Portable Risk Intelligence ("PRI") services for analysis and decision support. Qont does not sell, share, or misuse data in any form.

2) Role and Responsibility

Qont acts as both a data controller and data processor:

1. As controller, for managing client accounts, billing, and platform security.
2. As processor, for handling information submitted through the PRI Cloud APIs.

Qont does not read, review, or manually inspect client data unless required by law or to prevent abuse.

3) Data We Process

Qont PRI Cloud may process:

1. **Account and contact details for billing and authentication.**
2. **API request content sent by clients (processed automatically).**
3. **Technical metadata for diagnostics, load management, and compliance.**

Data is used only to deliver services, maintain security, and meet legal requirements.

4) Data Retention

Data is stored only as long as necessary to process each API request.

Temporary storage may occur for diagnostics, compliance, or billing validation.

All active or residual data is deleted automatically after processing or upon contract termination, unless required by law.

5) Security and Acces

Qont maintains strict internal controls.

All data is encrypted in transit and at rest.

Access is limited to authorized Qont personnel and automated systems.

Qont does not manually view, copy, or interact with client data, except when legally required or during verified abuse investigations.

6) Data Location and Transfers

Qont PRI Cloud may operate across multiple secure data centers worldwide.

All regions follow identical Qont privacy and encryption standards.

Data transfers between regions remain protected under Swiss and international data protection principles.

7) Law Enforcement and Legal Requests

Qont will only disclose data to law enforcement when required by valid legal process.

All such disclosures are logged and reviewed internally.

Qont does not provide voluntary data access or government backdoors.

8) Client Responsibilities

Clients using Qont PRI Cloud must ensure they have lawful consent or another legal basis to send data through Qont systems.

Qont accepts no responsibility for unauthorized or unlawful submissions made by clients.

9) Data Deletion on Request

Clients may request deletion of identifiable account data, logs, or stored records by contacting privacy@qont.net.

Deletion may be delayed if data is under legal review, tied to billing, or part of an active investigation.

10) Third Parties and Infrastructure Providers

Qont does not share data with external parties other than essential infrastructure or compliance providers.

All such partners operate under strict contractual confidentiality and data protection standards.

11) Data Transfers and Cross-Border Protection

Data may move between operational regions for processing or redundancy.

All transfers remain encrypted and compliant with Swiss privacy requirements.

Regional storage differences do not affect your data rights or protections.

12) Rights and Access Requests

You may request:

1. Access to information Qont holds about your organization.
2. Correction of inaccurate details.
3. Deletion of personal or account information.

Requests must be submitted in writing to privacy@qont.net and may require identity verification.

13) Business Use and Age Restriction

Qont PRI Cloud is for business, institutional, and professional use only.

It is not intended for individuals under 18 or for consumer-level data collection.

14) Compliance and Misuse

Qont does not get involved in client data or activities unless illegal use, fraud, or abuse is detected.

Any verified illegal use may result in immediate access termination and reporting to relevant authorities.

15) Governing Law and Disputes

This policy is governed by Swiss law.

All disputes or compliance matters shall be handled exclusively in Switzerland.

Data Processing Agreement (DPA)

1) Overview

This Data Processing Agreement ("DPA") forms part of the Terms of Service governing access to Qont PRI Cloud, a professional risk-intelligence infrastructure owned and operated by Qont.

This DPA applies automatically to all clients, developers, and organizations using the Qont PRI Cloud APIs.

By using Qont PRI Cloud, the client ("Controller") authorizes Qont ("Processor") to process submitted data strictly as described in this agreement.

2) Roles of the Parties

1. Client as Controller: Determines the purpose and means of processing the data sent through Qont PRI Cloud.
2. Qont as Processor: Processes data solely under the Controller's instruction, as required for service delivery, diagnostics, or lawful compliance.

Qont never uses data for unrelated purposes, profiling, or commercial exploitation.

3) Scope and Purpose of Processing

Qont processes data to:

1. Provide access to the Qont PRI Cloud APIs and related PRI services.
2. Maintain, diagnose, and secure system operations.
3. Comply with legal, billing, or audit requirements.

Data is not used for model training, resale, advertising, or analytics beyond operational metrics.

4) Use of Sub-Processors

Qont may engage trusted sub-processors (such as hosting or billing providers) under strict contractual confidentiality.

All sub-processors operate under equivalent privacy, security, and compliance obligations.

Qont remains responsible for all processing performed by its sub-processors.

5) Data Access and Security

Access to personal or client data is limited to authorized Qont personnel only when necessary for maintenance, debugging, or compliance review.

Security measures include encryption, access control, and activity logging in all environments.

Qont maintains continuous internal oversight to prevent unauthorized access or disclosure.

6) Data Retention and Deletion

All transmitted data is stored only for the duration required to process API requests or fulfill contractual obligations.

Data is automatically deleted or anonymized once processing is complete, unless retention is required by law, billing validation, or security investigation.

Upon service termination, Qont deletes or anonymizes all remaining data.

7) Data Breach Notification

In the event of a confirmed data breach involving client data, Qont will notify affected clients without undue delay after becoming aware of the incident.

Notifications include relevant details, scope, and corrective actions taken.

8) Data Transfers and Location

Data may be processed or stored in multiple secure data centers operated by or on behalf of Qont.

All transfers remain protected under Swiss privacy standards and encryption protocols.

Cross-border movement does not reduce client rights or security safeguards.

9) Client Responsibilities

The client is responsible for:

1. Ensuring lawful collection and transfer of data to Qont PRI Cloud.
2. Obtaining valid consent or another legal basis for all data sent.
3. Ensuring no prohibited or unlawful data types are transmitted.

Qont accepts no liability for data provided without lawful authority.

10) Law Enforcement and Disclosure

Qont does not grant voluntary access to any authority or third party.

Data will be disclosed only when required by valid legal process and with written documentation.

Where legally permitted, Qont will notify the client before releasing any data.

11) Data Subject Rights

If Qont receives a lawful request from an individual seeking access, correction, or deletion of data processed under this DPA, Qont will promptly notify the client and assist in fulfilling the request as required by law.

12) Security Overview

Qont maintains technical and organizational safeguards appropriate to the nature of data processed.

These include controlled access, encrypted storage and transmission, audit logging, and continuous risk evaluation.

Further details may be provided upon written request for compliance review.

13) Termination

Upon termination of service or expiration of a contract, Qont deletes or irreversibly anonymizes all client data unless retention is legally required.

Qont may retain non-identifiable operational logs for auditing and service continuity.

14) Liability

Qont's liability under this DPA is limited to direct damages proven to result from Qont's own negligence or breach.

Qont is not liable for indirect, consequential, or client-caused losses.

15) Governing Law and Jurisdiction

This DPA is governed by Swiss law, except where a region-specific agreement states otherwise.

All disputes or enforcement actions shall be handled exclusively under Swiss jurisdiction unless otherwise defined in the client's main contract.

Acceptable Use Policy (AUP)

1) Overview

This Acceptable Use Policy ("Policy") defines permitted and prohibited uses of the Qont PRI Cloud platform and its associated APIs.

It applies to all clients, developers, organizations, and any recipient of Qont PRI Cloud data or functionality ("Users").

By accessing or using Qont PRI Cloud, Users agree to comply with this Policy and all applicable laws.

2) Proper Use of Qont PRI Cloud

Qont PRI Cloud provides licensed access to Portable Risk Intelligence (PRI) through secure APIs.

Users may submit data and retrieve risk outputs solely for lawful business or analytical purposes under their contract or agreement with Qont.

All API keys, credentials, and access details must be kept confidential and protected from unauthorized use.

3) Prohibited Activities

Users must not:

1. Reverse engineer, replicate, benchmark, or repackage any part of Qont PRI Cloud, its data, or logic.
2. Use PRI outputs or APIs for unlawful, fraudulent, harmful, or unethical activity.
3. Transmit data for surveillance, discrimination, or manipulation of individuals or entities.
4. Automate excessive or abusive API calls beyond assigned rate limits or contractual capacity.
5. Obscure, alter, or falsify Qont PRI Cloud outputs when displayed or distributed.
6. Misrepresent association, partnership, or endorsement by Qont in any form.

4) Data Responsibility

Users are fully responsible for all data they transmit through Qont PRI Cloud, including personal, medical, or financial data.

Qont does not control or validate the legality, accuracy, or ethical use of submitted data or resulting outputs.

Users must ensure that all submissions comply with their own local laws and data protection obligations.

5) Security Obligations

Users must:

1. Keep API keys, credentials, and access tokens secure at all times.
2. Report any unauthorized access or suspected compromise immediately to report@qont.net.
3. Qont reserves the right to disable or reset credentials following any confirmed security risk.

6) Monitoring and Enforcement

Qont monitors API activity for abuse, fraud, or policy violations.

Logs may be reviewed for compliance and integrity assurance.

Qont may suspend or permanently revoke access at any time if a violation is detected or suspected.

No refund or credit will be issued in cases of breach or misuse.

7) Compliance and Local Law

Users are solely responsible for ensuring compliance with all applicable local laws, privacy rules, and export controls related to their use of Qont PRI Cloud.

Use of the PRI Cloud does not exempt Users from their own regional or legal obligations.

8) Content and Output Integrity

All PRI outputs must remain accurate and unmodified.

Users may not distort, conceal, or edit results to misrepresent findings or mislead others.

Qont retains full control over the authenticity and definition of PRI data.

9) Non-Affiliation

Use of Qont PRI Cloud does not imply partnership, sponsorship, or endorsement by Qont.

Users may not use Qont's name, logo, or trademarks without written authorization.

10) Violation and Reporting

Violations of this Policy should be reported immediately to:

Email: report@qont.net

Website: qont.net/report

Qont investigates all credible reports and reserves the right to take any lawful action to protect its systems and reputation.

11) Enforcement and Termination

Qont may suspend or terminate any account or integration that violates this Policy or poses operational, legal, or reputational risk.

All terminations are final and non-reversible.

12) Governing Law

This Policy is governed by Swiss law, except where regional contract terms specify otherwise.

API License Agreement

1) Overview

This API License Agreement ("Agreement") governs access to and use of the Qont PRI Cloud application programming interfaces ("APIs") provided by Qont.

By activating or using an API key, the recipient ("Licensee") agrees to these terms.

The Qont PRI Cloud APIs enable access to Portable Risk Intelligence ("PRI") services and data streams for approved business, enterprise, and developer use.

2) License Grant

Qont grants each Licensee a limited, non-exclusive, non-transferable, revocable license to access and use the Qont PRI Cloud APIs strictly for their authorized business operations.

This license allows Licensees to call, integrate, and display PRI outputs within internal or customer-facing systems in accordance with this Agreement.

No ownership, intellectual property, or source rights are transferred.

All Qont technology, frameworks, and datasets remain the exclusive property of Qont.

3) Use Conditions

Licensees may integrate PRI outputs within approved applications or dashboards, provided that:

1. The system displays attribution as "Powered by Qont PRI Cloud" or equivalent wording.
2. PRI data is not resold, redistributed, or presented as an independent product.
3. PRI Cloud technology remains the sole active PRI framework in all machines or systems using it.

Competitors may license and use Qont PRI Cloud, but must not replicate or embed competing PRI frameworks or derivative engines.

4) Data Handling and Confidentiality

Licensees must protect all API keys, documentation, and output data.

Access credentials may not be shared, transferred, or exposed to the public.

All data exchanged through Qont PRI Cloud must remain confidential unless already public or expressly authorized by Qont.

5) Revocation and Termination

Qont reserves the right to suspend or revoke API access at any time for misuse, security risk, or contractual breach.

Upon termination of the account, license, or subscription:

1. **All usage rights end immediately.**
2. **All stored credentials, data, and API outputs must be permanently deleted.**

Continued use after termination constitutes unauthorized access.

6) Billing and Audit

Qont monitors API usage for volume, rate, and compliance.

Licensees agree to periodic review of their usage data for billing and audit purposes.

Any discrepancies or excess usage beyond contractual terms may result in adjustment or suspension.

7) Service Modifications

Qont may update, change, or deprecate any API endpoint, authentication process, or documentation at any time.

Reasonable notice will be provided to active Licensees before major service changes.

8) Liability and Warranty

The Qont PRI Cloud APIs are provided "as is."

Qont makes no guarantee of uptime, accuracy, or suitability for any specific use.

Qont is not liable for indirect, incidental, or consequential damages, including loss of revenue, data, or business opportunity.

9) Compliance

Licensees must comply with all applicable laws, export restrictions, and security obligations related to their use of Qont PRI Cloud.

Qont assumes no responsibility for Licensee data handling outside its systems.

10) Attribution

All public or commercial interfaces using Qont PRI Cloud outputs must clearly display the attribution "Powered by Qont PRI Cloud" or an approved equivalent.

Failure to maintain proper attribution constitutes a breach of this Agreement.

11) Ownership and Intellectual Property

All rights, titles, and interests in Qont's PRI logic, datasets, and framework architecture remain vested in Qont.

Licensees receive access only under limited license terms and may not claim ownership or derivative authorship.

12) Governing Law and Disputes

This Agreement is governed by Swiss law.

All disputes arising under or related to this Agreement shall be resolved under Swiss jurisdiction unless an individual contract defines an alternate region.

Service Level Agreement (SLA)

1) Overview

This Service Level Agreement ("SLA") outlines the service reliability, operational standards, and client support expectations for Qont PRI Cloud, owned and operated by Qont.

It applies to all approved clients and organizations using Qont PRI Cloud APIs and related infrastructure.

By using Qont PRI Cloud, clients agree to these terms as part of their overall service contract.

2) Service Reliability

Qont PRI Cloud is built on a high-reliability, globally distributed infrastructure.

While Qont aims to provide continuous access, service performance may vary by region, network conditions, or client integration.

Uninterrupted uptime is not guaranteed.

3) Maintenance and Updates

Scheduled maintenance, updates, or system improvements may cause temporary interruptions.

Qont provides reasonable advance notice to affected clients whenever operationally possible.

Urgent maintenance for security or stability may occur without prior notice when required.

4) Monitoring and Performance

Qont continuously monitors its PRI Cloud systems for uptime, stability, and performance across all active regions.

Operational data is reviewed regularly to ensure reliability and detect anomalies before service impact.

5) Support Availability

Direct support lines are provided to all approved clients.

Each client receives access to their assigned Qont support contact for operational assistance and account-specific queries.

Response priority is determined by the client's contractual tier and the severity of the issue.

6) Incident Reporting and Communication

Clients may report service incidents or performance issues through their assigned line or at qont.net/status.

Qont provides timely updates during investigations and will confirm resolution once stability is restored.

7) Priority Response and Escalation

Qont prioritizes incidents that affect multiple clients or core PRI Cloud functionality.

Confirmed issues receive immediate corrective attention, and clients may request escalation through their dedicated support contact.

8) Data Integrity and Processing

Qont ensures data accuracy and security within its controlled systems.

Qont is not responsible for errors caused by client-submitted data, misuse, or external system dependencies.

9) Limitations and Disclaimers

Qont is not responsible for service interruptions, delays, or degraded performance resulting from:

1. Internet or connectivity failures outside Qont's control.
2. Third-party infrastructure, integrations, or client systems.
3. Force majeure events or regulatory actions.

All services are provided "as available."

10) Remediation and Corrective Action

When Qont confirms a service issue within its control, corrective measures are implemented as soon as reasonably possible.

Clients are notified once remediation is complete or if additional action is required on their end.

11) No Credit Policy

Qont PRI Cloud operates on a reliability-based model.

No financial or service credits are issued for downtime, latency, or interruptions.

12) Termination and Continuation

Upon termination of service, Qont retains limited technical logs for verification and audit purposes.

No uptime or support obligations apply after termination.

All client access credentials will be disabled, and residual data will be deleted per Qont's Data Processing Agreement.

Cloud Security Policy

1) Overview

This Cloud Security Policy describes the technical, operational, and procedural safeguards maintained by Qont to protect all systems and data processed through Qont PRI Cloud.

It applies globally across all Qont infrastructure, services, and APIs.

While Qont cannot guarantee absolute security, it maintains robust controls and practices to protect data to the best of its ability.

2) Infrastructure Control

Qont operates and manages its own private infrastructure, supported by selected and vetted service providers where necessary.

All systems are maintained under Qont's direct oversight and are secured through layered access, monitoring, and operational controls.

3) Data Protection and Storage

Qont safeguards all data processed through PRI Cloud using industry-standard methods for protection in transit and at rest.

Encryption and access safeguards are applied to the highest feasible standard at all times.

Encryption keys and configurations remain under Qont's exclusive control.

4) Data Isolation and Access Control

Each client's data is logically separated within the Qont PRI Cloud environment.

Access to systems is strictly limited to authorized Qont personnel and only granted when necessary for maintenance, diagnostics, or verified lawful investigations.

All access is logged and reviewed.

5) Security Monitoring and Detection

Qont continuously monitors its infrastructure to detect unauthorized access, misuse, or anomalies.

Any suspicious or abnormal activity is investigated immediately, and corrective measures are taken as required.

6) Vulnerability Management and Patching

Qont regularly updates its infrastructure, dependencies, and libraries to mitigate exposure to known security threats.

Security patches and system upgrades are applied on a scheduled basis, with emergency updates deployed as soon as practical.

7) Lawful Access

Qont may access or disclose data only when required by law, court order, or verified regulatory process.

Data will never be accessed or shared voluntarily or without lawful basis.

8) Client Responsibility

Clients are responsible for maintaining security on their own systems, networks, and integrations connected to Qont PRI Cloud.

This includes securing API keys, credentials, and endpoint configurations.

Qont does not manage or monitor client-side systems.

9) Third-Party Infrastructure

Qont may rely on limited third-party data centers, monitoring tools, or compliance systems.

All providers are vetted for reliability, security, and adherence to Qont's privacy and operational standards.

Qont remains fully responsible for their performance.

10) Data Retention and Disposal

Data is retained only for as long as required to fulfill operational, compliance, or maintenance needs.

When no longer necessary, data is securely deleted or anonymized following internal disposal procedures.

11) Breach Response and Reporting

If a security breach is confirmed, Qont will investigate immediately and notify affected clients within a reasonable period after verification.

Corrective actions are implemented to restore system integrity and prevent recurrence.

12) Compliance and Audit

Qont periodically reviews its infrastructure and security processes to ensure alignment with Swiss, EU, and comparable data protection frameworks.

Independent or internal audits may be conducted to verify compliance with this policy.

13) Service Continuity and Recovery

Qont maintains redundant systems and backup processes to ensure operational continuity in case of regional outages or failures.

Recovery procedures are tested periodically to confirm service resilience.

Export Control & Global Trade Compliance Policy

1) Overview

This Export Control & Global Trade Compliance Policy ("Policy") defines the export, re-export, and lawful use requirements for Qont PRI Cloud, owned and operated by Qont.

It applies to all clients, developers, partners, and distributors worldwide.

By accessing or using Qont PRI Cloud, all parties agree to comply with applicable international trade, export, and sanctions regulations.

2) Legal Framework

Qont operates under the export control laws of Switzerland, alongside applicable European Union, United Nations, and United States regulations.

All users must comply with their own regional trade, customs, and export laws.

This includes ensuring that Qont PRI Cloud is not used, sold, transferred, or made available in violation of any international embargo, sanctions program, or restricted country listing.

3) Restricted Regions and Prohibited Transfers

Qont PRI Cloud must not be exported, resold, or deployed in countries or regions subject to United Nations, Swiss, EU, or U.S. embargoes or sanctions.

No user may transfer or sublicense Qont PRI Cloud access, API keys, or derived technologies to a third party without Qont's prior written approval.

4) Licensed and Authorized Use

Certain advanced or defense-capable applications of Qont PRI Cloud may be licensed for use by verified military or government contractors.

These entities must receive written authorization from Qont before integration, deployment, or distribution.

All such authorizations are issued under strict contractual control, traceability, and compliance verification.

Unauthorized military or surveillance use is prohibited.

5) Responsibility and Liability

Clients and partners are fully responsible for ensuring compliance with all applicable export, import, and trade laws in their jurisdiction.

Qont assumes no liability for violations caused by client-side export or resale activities.

6) Reporting and Verification

Clients must immediately notify Qont if they become aware of, suspect, or are involved in any activity that could constitute a violation of export or sanctions regulations.

Notifications should be directed to compliance@qont.net.

Qont may request supporting documentation or confirmation of corrective actions.

7) Trade Documentation and Audit

Qont reserves the right to verify compliance with this Policy and request evidence such as export licenses, import records, or end-user certificates.

Clients and partners must cooperate fully and provide relevant records upon request for compliance or regulatory review.

8) Cooperation with Authorities

All clients, distributors, and contractors agree to cooperate with Qont and authorized regulators in any export control audit, inspection, or investigation.

This includes providing accurate information and timely responses as required by law.

9) Enforcement and Penalties

Qont may suspend or terminate access to PRI Cloud immediately if a user, partner, or organization is found — or reasonably suspected — to be in violation of this Policy or any applicable trade regulation.

Qont may also report such incidents to appropriate authorities when legally required.

Intellectual Property & Confidentiality Policy

1) Overview

This Intellectual Property & Confidentiality Policy ("Policy") defines ownership, usage rights, and confidentiality obligations related to Qont PRI Cloud, owned and operated by Qont.

It applies to all clients, developers, contractors, and partners who access or use Qont PRI Cloud, its APIs, or any associated services.

2) Ownership and Intellectual Property

All technologies, algorithms, frameworks, datasets, visual materials, and documentation within Qont PRI Cloud are exclusive intellectual property of Qont.

No ownership, title, or proprietary interest is transferred to any user, partner, or organization through access, contract, or integration.

Qont retains full control over all intellectual property derived from its systems, regardless of use context or distribution channel.

3) Limited License of Use

Clients and partners are granted a limited, non-exclusive, non-transferable license to use PRI outputs and services strictly for approved purposes.

No Qont product, dataset, or API output may be resold, reproduced, sublicensed, or represented as an independent system.

Any derivative or public use of Qont-generated data must acknowledge Qont as the originating source.

4) Confidential Information

"Confidential Information" includes all non-public information disclosed by Qont or its clients, including data, documentation, technical processes, pricing, client details, business plans, and operational insights.

All parties must maintain strict confidentiality and prevent unauthorized disclosure, duplication, or distribution.

Disclosure is permitted only with written consent from the disclosing party.

5) Mutual Confidentiality

Qont treats all client-provided data, materials, and system information as confidential.

Such information is used solely for the purpose of service delivery, technical support, or compliance with legal obligations.

Qont does not sell, trade, or share confidential data with third parties.

6) Restricted Use and Non-Competition

Clients, partners, and contractors may not:

1. Reverse-engineer or reproduce any Qont system or algorithm.
2. Develop competing risk-intelligence or analytics technology based on Qont materials.
3. Use confidential knowledge or access credentials to replicate Qont's intellectual property or data models.

7) Retention and Return of Materials

All Qont-owned materials, credentials, and documentation must be securely deleted or returned upon termination of access, contract expiration, or written request.

Qont reserves the right to verify deletion or return compliance.

8) Attribution and Credit

Any reference to Qont technology or materials in public or private communications must use the correct and approved name: "Qont" or "Qont PRI Cloud."

No user, partner, or affiliate may alter, obscure, or rebrand Qont identifiers or marks.

All attributions must remain factual and non-promotional.

9) Breach and Remedies

Violation of this Policy may result in immediate suspension of access, termination of agreements, or legal action.

Qont reserves the right to pursue all available remedies, including injunctive relief and financial recovery, in the event of intellectual property misuse or unauthorized disclosure.

10) Duration of Confidentiality

All confidentiality obligations under this Policy remain in effect during the course of use and for five (5) years following the termination or expiration of any related contract or license.

Branding & Co-Marketing Guidelines

1) Overview

These Branding & Co-Marketing Guidelines ("Guidelines") govern the public and promotional use of Qont and Qont PRI Cloud brand assets by approved clients, partners, and contractors.

They apply to all references, marketing activities, and integrations where Qont or its technologies are represented.

By using Qont's brand assets, all parties agree to follow these Guidelines and applicable laws.

2) Approved Users

Branding privileges are available to:

1. **Verified clients and integration partners.**
2. **Approved military or enterprise contractors under written license.**
3. **Resellers or affiliates authorized through Qont's official programs.**

All others must obtain prior written approval before using Qont trademarks or brand references.

3) Brand Assets and Availability

Official Qont logos, badges, and marks can be found at qont.net/media-kit, through Qont PRI Cloud documentation, or provided directly during activation.

Only these official assets may be used.

They must not be altered, recolored, distorted, or animated.

Qont logos must always remain clear, legible, and unmodified.

4) Required Attribution

When Qont PRI Cloud powers a product, service, or display, the phrase "Powered by Qont PRI Cloud" must appear alongside the official badge provided by Qont.

Attribution must follow these standards:

1. **The logo must be at least equal in size to the body text surrounding it.**
2. **It must not be smaller than 10 px in digital format.**
3. **It must maintain clear space equal to at least the height of the letter "Q" around all sides.**
4. **Placement should be on a neutral background and never obscured or stylized.**

5) Visual Standards

Qont brand assets must appear on a white, black, or Titanium Grey background only.

They must never be placed over gradients, photographs, or patterned surfaces.

Do not combine Qont assets with any other brand marks, nor apply shadows, outlines, or effects.

6) Co-Marketing and Joint Promotions

Partners may request approval to reference Qont PRI Cloud in joint marketing, case studies, or media releases.

All materials must be submitted to Qont for review and written approval before publication.

Approved co-marketing must remain factual, professional, and accurately represent Qont technology.

7) Tone and Representation

Any mention of Qont or Qont PRI Cloud must be neutral and factual.

Do not make exaggerated claims, promotional comparisons, or technical assumptions.

All representations must align with Qont's professional tone and ethical standards.

8) Naming Protection

No party may use "Qont," "PRI," "PRI Cloud," or any similar mark within product names, domains, or company branding without explicit written authorization from Qont.

This restriction includes subdomains, app titles, and derivative branding.

9) Marketing Conduct

Partners and clients may not imply endorsement, ownership, or exclusive relationship with Qont.

All branding and references must indicate that the integration or service is powered by Qont PRI Cloud — not owned or managed by Qont unless otherwise agreed.

10) Revocation and Enforcement

Qont reserves the right to revoke brand-use permissions or disable asset access at any time for misuse, misrepresentation, or non-compliance.

All Qont brand assets remain the exclusive intellectual property of Qont.

Unauthorized use or imitation may result in suspension, termination, or legal action.
