Security Whitepaper

Plan d'Assurance Sécurité

PUBLIC

v2.0 - June 2025

Table of Content

Information Security Policy

Pennylane is a Software-as-a-Service combining production software for accountants and financial management tools for their clients.

Pennylane centralizes in real time all the financial flows of companies and facilitates the collaboration between managers and their accountants.

Due to the sensitive nature of its customers' data (accounting, financial, banking, personal data, etc.), Pennylane is dedicated to develop and maintain its products and operations according to strong and recognized standards for its Information Security Management System control and continual improvement, especially regarding its customers' data confidentiality.

This document is the public version of Pennylane's Information Security Policy (annually reviewed), structured under 6 main principles:

1. Compliance of the Information Security Management System (set of security policies and controls governing all assets and data), at all times and on each point, to ISO/IEC 27001.
2. Strict protection and control of data confidentiality, integrity and availability, through practices and mechanisms offering authorization, encryption, traceability, backup and a robust infrastructure.
3. Control, restriction and monitoring of all access to data by authorized employees and partners, in strict proportion to the need to know, according to both the applicable laws and the internal regulation.
4. General Data Protection Regulation (GDPR) compliance, through users' personal data processing lawfully, securely in relation to the data subject.
5. Continuous training of all employees and partners to best practices, for their daily contribution to information security.
6. Ensure operational resilience by remaining robust, adaptable and secure against disruptions, with effective incident management and reliable third-party relationships.

The compliance to ISO 27001, regularly audited both by internal auditors and external independent experts, was obtained in September 2023.

Arthur Waller

Co-founder and CEO of Pennylane

Politique de Sécurité de l'Information

Pennylane est un Software-as-a-Service combinant un logiciel de production pour les comptables et des outils de gestion financière pour leurs clients.

Pennylane centralise en temps réel tous les flux financiers des entreprises et facilite la collaboration entre les dirigeants et leurs comptables.

En raison de la nature sensible des données de ses clients (données comptables, financières, bancaires, personnelles, etc.), Pennylane s'engage à développer et à maintenir ses produits et opérations selon des normes fortes et reconnues de contrôle et d'amélioration continue de son Système de Gestion de la Sécurité de l'Information, notamment en ce qui concerne la confidentialité des données de ses clients.

Ce document est la version publique de la politique de sécurité de l'information de Pennylane (revue annuellement), structurée en 6 grands principes :

1. Conformité du système de management de la sécurité de l'information (ensemble de politiques et de contrôles de sécurité régissant tous les actifs et les données), à tout moment et en tout point, à la norme ISO/CEI 27001.
2. Protection et contrôles stricts de la confidentialité, de l'intégrité et de la disponibilité des données, au moyen de pratiques et de mécanismes d'autorisation, de chiffrement, de traçabilité, de sauvegarde et d'une infrastructure robuste.
3. Contrôle, restriction et surveillance de tous les accès aux données par les employés et partenaires autorisés, en stricte proportion avec le besoin d'en connaître, selon les lois applicables et le règlement interne.
4. Conformité au Règlement Général sur la Protection des Données (RGPD), par le traitement des données personnelles des utilisateurs de manière légale, sécurisée en rapport avec le type de donnée.
5. Formation continue de tous les employés et partenaires aux meilleures pratiques, et à leur contribution quotidienne à la sécurité de l'information.
6. Assurer la sécurité et la qualité de notre résilience opérationnelle, grâce à une gestion efficace des incidents et un contrôle régulier de nos sous-traitants.

La conformité à la norme ISO 27001, régulièrement vérifiée par des auditeurs internes et des experts indépendants externes, a été officiellement obtenue en septembre 2023.

Arthur Waller

Co-fondateur et CEO de Pennylane

ISO 27001, Risks and DORA

- Pennylane engagements and operations for information security are designed under the international ISO 27001:2022 standard and in compliance with all its provisions and controls (all 93 controls), for all its products, operations and sites present as to come.

  Les engagements et procédures de Pennylane en matière de sécurité de l'information sont conçus selon la norme internationale ISO 27001:2022, dans toutes ses dispositions et contrôles, pour tous ses produits, opérations et sites présents comme à venir.

  Pennylane has been certified against ISO 27001 since September 2023.

  Pennylane est certifiée selon la norme ISO 27001 depuis septembre 2023.

Certificate No 786660 / Validity from 2024-09-10 to 2026-09-19 (click to check)

Certificate in annex of the present document

- The compliance to ISO 27001 is regularly audited, both by internal auditors and external independent experts: BSI, a world leader in standards and certification operations, is the independent auditor of Pennylane.

  La conformité à la norme ISO 27001 est régulièrement auditée, tant par des auditeurs internes que par des experts externes indépendants : BSI, un des leaders mondiaux dans les opérations de normalisation et de certification, est l'auditeur indépendant de Pennylane.

- Pennylane demonstrates strong DORA (EU regulation for digital operational resilience in the financial sector) compliance through its resilience strategy, risk assessments, regular security independent assessment, and third-party management. An independent external audit revealed no major compliance gaps, while emphasizing Pennylane's mature approach to control design and documentation.

  Pennylane démontre une forte conformité au règlement DORA (règlement européen sur la résilience opérationnelle numérique du secteur financier) grâce à une stratégie de résilience, l'évaluation des risques, des contrôles de sécurité réguliers et indépendants, et une gestion des tiers. Un audit externe indépendant n'a révélé aucun écart majeur de conformité, tout en soulignant l'approche mature de Pennylane dans la conception et la documentation des contrôles.

- Pennylane assesses its risks, including those related to Information Security, through a process based on ISO 27005 principles, for assessment, treatment plan with internal operations experts, regular monitoring and continual improvement through a dedicated team and the support of the senior management team.

  Pennylane évalue ses risques, y compris ceux liés à la sécurité de l'information, par un processus basé sur les principes de la norme ISO 27005, pour l'évaluation, le plan de traitement avec les experts internes dans chaque domaine, le suivi régulier et l'amélioration continue par une équipe dédiée et avec le soutien de l'équipe de direction.

- Pennylane effectively implements its mission statement for a strong and continuous level of information security in all its operations, through a set of practical and controlled policies (internally restricted), annually reviewed, designed and evaluated under the review of the Executive Committee of C-level management.

  Pennylane met effectivement en œuvre son engagement pour un niveau fort et continu de sécurité de l'information dans toutes ses opérations, grâce à un ensemble de politiques pratiques et contrôlées (à diffusion interne restreinte), revues, conçues et évaluées annuellement sous le contrôle du Comité Exécutif.

People

- Pennylane maintains a dedicated security team and a dedicated legal team, both referring to the Executive Committee of C-level management, for design and performance review.

  Pennylane dispose d'une équipe de sécurité dédiée et d'une équipe juridique dédiée, toutes deux référant au Comité Exécutif, pour la conception et l'examen des performances.

- All employees are trained to internal regulation on confidentiality and security at least once a year, including on procedures to report security incidents. Pennylane continually performs phishing campaigns for training all employees.

  Tous les employés sont formés au règlement interne sur la confidentialité et la sécurité au moins une fois par an, y compris sur les procédures de signalement des incidents de sécurité. Pennylane réalise en permanence des campagnes de phishing pour former tous les employés.

- All employees are required to work under strict confidentiality and nondisclosure clauses.

  Tous les employés sont tenus de travailler dans le cadre de clauses strictes de confidentialité et de non-divulgation.

- All employees and external contractors are required to follow a global internal regulation on daily security and privacy rules and best practices. This regulation particularly designs the rules for teleworking, data usage, software use and procurement, messaging and information classification, etc.

  Tous les employés et les contractants externes sont tenus de suivre un règlement interne global sur les règles et les meilleures pratiques quotidiennes en matière de sécurité et de confidentialité. Ce règlement prévoit notamment les règles de télétravail, d'utilisation des données, d'utilisation et d'acquisition de logiciels, de messagerie et de classification des informations, etc.

- Pennylane works to check candidates' background on past professional experiences and qualifications, according to the law.

  Pennylane travaille à vérifier les antécédents des candidats, sur leurs expériences professionnelles passées et leurs qualifications, conformément à la loi.

- Pennylane employees are requested to reserve any printing to absolute necessity, to lock their computer when away, to maintain their desk clear from any confidential information.

  Les employés de Pennylane doivent réserver toute impression aux absolues nécessités, verrouiller leur ordinateur en cas d'absence, maintenir leur bureau libre de toute information confidentielle.

Data, Banking, Hosting, Encryption

- All data, including backups, are stored in Ireland by Amazon Web Services, in respect of ISO 27001 and SOC2 norms, among other certifications. As an exception, data related to France's electronic invoicing (PDP) frame are stored by 3DS Outscale in France, in compliance with ISO 27001 and SecNumCloud 3.2, among other certifications.

  Toutes les données, y compris les sauvegardes, sont stockées en Irlande par Amazon Web Services, dans le respect des normes ISO 27001 et SOC2, entre autres certifications. Par exception, les données liées au cadre de la facturation électronique (PDP) en France sont stockées par 3DS Outscale en France, en conformité avec les normes ISO 27001 et SecNumCloud 3.2, entre autres certifications.

- All data are encrypted both in transit (TLS 1.2/1.3 with HSTS and Perfect Forward Secrecy fully enabled) and at rest (AES-256-GCM and BCrypt).

  Toutes les données sont chiffrées en transit (TLS 1.2/1.3 avec HSTS et Perfect Forward Secrecy entièrement activé) et au repos (AES-256-GCM et BCrypt).

- Additionally, Pennylane encrypts the most sensitive data a second time before any hosting at rest. The opportunity and necessity of such encryption, for new documents and old ones, is controlled each month, as part of the centralized internal audit program.

  En supplément, Pennylane chiffre une seconde fois les données les plus sensibles avant tout hébergement au repos. L'opportunité et la nécessité de ce chiffrement, pour les nouveaux documents comme pour les anciens, sont contrôlées chaque mois, dans le cadre du programme d'audit interne centralisé.

- All application files are securely stored in versioned environments. Access to the files is granted through a pre-signed secure link, generated by the application's permission system.

  Tous les fichiers de l'application sont stockés chiffrés dans des environnements versionnés. L'accès aux fichiers se fait via un lien pré-signé sécurisé, généré par le mécanisme de permissions de l'application.

- Pennylane offers a secure connection to users' bank accounts using several methods, tailored to the specificities of each bank: either through OAuth2 (safe and convenient way for users to grant third-party applications access) or through the services of Bridge and Powens (ACPR/DSP2 compliant and renowned leaders in the French open-banking sector).

  Pennylane offre une connexion sécurisée aux comptes bancaires des utilisateurs en utilisant plusieurs méthodes, adaptées aux spécificités de chaque banque : soit par le biais de OAuth2 (un moyen sûr et pratique pour les utilisateurs d'accorder l'accès aux applications tierces) ou par le biais des services de Bridge et Powens (conformes à l'ACPR/DSP2 et leaders reconnus dans le secteur de l'open-banking français).

- Pennylane also employs the EBICS protocol with various service providers. EBICS (Electronic Banking Internet Communication Standard) is a secure, Internet-based communication standard used by banks, offering high levels of security and proper access control.

  Pennylane utilise également le protocole EBICS avec divers fournisseurs de services. EBICS (Electronic Banking Internet Communication Standard) est un standard de communication sécurisé basé sur Internet utilisé par les banques, offrant des niveaux élevés de sécurité et un contrôle d'accès approprié.

- In parallel to its ISO 27001 certification for all its activities and products, Pennylane complies with the rigorous requirements of Prudential Control and Resolution Authority (ACPR, Banque de France) regulations and is accredited as an account information service provider.

  En parallèle à sa certification ISO 27001 pour toutes ses activités et produits, Pennylane se conforme aux exigences rigoureuses de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR, Banque de France), auprès de laquelle elle est accréditée en tant que fournisseur de service d'information sur les comptes.

- All users of Pennylane application must authenticate themselves by email and password controlled by a strict quality policy, with a different mandatory secondary factor of authentication (SMS or push-app notification or external security key). Pennylane employees are requested to use the corporate Single Sign On, with mandatory second factor of authentication. The login on Pennylane is limited to a strict limit of attempts with lock capabilities, requesting Pennylane employees validation for lifting accounts security lockdown.

  Tous les utilisateurs de l'application Pennylane doivent s'authentifier par email et un mot de passe contrôlé par une politique de qualité stricte, avec un facteur d'authentification secondaire obligatoire différent (SMS ou notification push-app ou clef de sécurité externe). Les employés de Pennylane doivent utiliser le système d'authentification unique de l'entreprise, avec un second facteur d'authentification obligatoire. La connexion sur Pennylane est limitée à un nombre strict de tentatives avec des capacités de verrouillage, demandant la validation des employés de Pennylane pour lever le verrouillage de sécurité des comptes.

- All employees' access are centrally managed by a dedicated team, enforcing the principle of least privilege to guarantee that each employee has only the necessary rights for the success of their mission and only for its duration. Regular audits are controlling the effectiveness of this policy.

  Les accès de tous les employés sont gérés de manière centralisée par une équipe dédiée, qui applique le principe du moindre privilège afin de garantir que chaque employé ne dispose que des droits nécessaires au succès de sa mission et uniquement pour sa durée. Des audits réguliers contrôlent l'efficacité de cette politique.

- Pennylane employees authorized to access customer data, only for support or technical development, must request the user's consent or justify their reason to do so. All data modifications are logged and regularly audited for internal compliance and conformity.

  Les employés de Pennylane autorisés à accéder aux données des clients, uniquement à des fins de support ou de développement technique, doivent obtenir le consentement de l'utilisateur ou justifier de leurs raisons. Toutes les modifications de données sont enregistrées et font l'objet d'un audit régulier de conformité interne.

- A global review of data access, for auditing against users' roles and rights matrix, is carried out each month as part of the centralized internal audit program.

  Un examen global de l'accès aux données, pour vérification par rapport à la matrice des rôles et des droits des utilisateurs, est effectué chaque mois dans le cadre du programme d'audit interne centralisé.

Premises

- Access to Pennylane's premises requires individual identification 24/7/365, at a guarded reception on ground entrance and at each floor.

  L'accès aux locaux de Pennylane nécessite une identification individuelle 24/7/365, à une réception gardée au rez-de-chaussée, comme à chaque étage.

- All visitors should log themselves and be accompanied at all times.

  Tous les visiteurs doivent s'enregistrer et être accompagnés en permanence.

- Premises are monitored 24/7/365 by a video-surveillance system, with alarm capabilities out of office hours.

  Les locaux sont surveillés 24/7/365 par un système de vidéosurveillance, avec des capacités d'alarme en dehors des heures d'ouverture.

Assets, Suppliers

- All devices are centrally managed by strict policies ensuring disk encryption, firewall enabling, screen auto-lock, password quality and rotation, protection against malware, updates, remote device lock and erase capabilities.

  Tous les appareils sont administrés de manière centralisée par des politiques strictes garantissant le chiffrement des disques, l'activation du pare-feu, le verrouillage automatique de l'écran, la qualité et la rotation des mots de passe, la protection contre les logiciels malveillants, les mises à jour, le verrouillage et l'effacement des appareils à distance.

- All devices are running an Endpoint Detection and Response software, to check conformity, to counter malware, to detect and to block specific threats.

  Tous les appareils utilisent un logiciel de détection et de réponse (EDR), pour vérifier la conformité, contrer les logiciels malveillants, détecter et bloquer des menaces spécifiques.

- All employees are logging themselves daily to any software (few controlled exceptions, never on critical software, managed through mandatory password manager) thanks to a corporate managed Single Sign On (SSO), with strict password quality (entropy, maximum age) requirements and a second factor of authentication (2FA), allowing to restrict login capabilities and to audit employees' access rights.

  Tous les employés se connectent quotidiennement à tout logiciel (quelques exceptions contrôlées, jamais sur des logiciels critiques, gérées par un gestionnaire de mots de passe obligatoire) grâce à un système d'authentification unique (SSO) géré par l'entreprise, avec des exigences strictes en matière de qualité des mots de passe (entropie, âge maximum) et un second facteur d'authentification (2FA), permettant de restreindre les capacités de connexion et d'auditer les droits d'accès des employés.

- Software are globally listed and managed, for authorization to use according to data type and information classification.

  Les logiciels sont répertoriés et gérés globalement, pour une autorisation d'utilisation selon le type de données et la classification des informations traitées.

- All employees' professional data must be stored online on Pennylane storage providers, for automatic and continuous backup.

  Toutes les données professionnelles des employés doivent être stockées en ligne sur les fournisseurs de stockage de Pennylane, pour une sauvegarde automatique et continue.

- All access and rights, as accounts themselves, are regularly audited by the security / IT team, against business needs and employees onboarding / offboarding.

  Tous les accès et droits, ainsi que les comptes eux-mêmes, sont régulièrement audités par l'équipe Security / IT, selon les besoins des missions, comme l'état des entrées et sorties des employés.

- All external media are by default banned.

  Tous les périphériques externes de stockage sont interdits par défaut.

- Pennylane deploys a procedure for all providers (software tooling, as external professionals working on data) procurement validation, including a mandatory joint security, legal, finance clearance.

  Pennylane suit une procédure de validation des achats de tous les fournisseurs (outils logiciels, comme professionnels externes travaillant sur les données), incluant une validation conjointe obligatoire de sécurité, juridique et financière.

- Specific contractual provisions, whenever possible, are allowing Pennylane to audit the continuity and efficiency of its suppliers' security policies and controls, especially regarding confidentiality, SLAs, internal regulation and security measures, legal evolutions, obligations regarding data privacy regulation.

  Des dispositions contractuelles spécifiques, dans la mesure du possible, permettent à Pennylane de vérifier la continuité et l'efficacité des politiques et des contrôles de sécurité de ses fournisseurs, notamment en ce qui concerne la confidentialité, les accords de niveau de service, la réglementation interne et les mesures de sécurité, les évolutions légales, les obligations en matière de réglementation de la confidentialité des données.

Development

- All accesses and modifications of the source code are strictly controlled by automatic procedures and reviewed by peers.

  Tous les accès et modifications du code source sont strictement contrôlés par des procédures automatiques et revus par des pairs.

- All Pennylane platform APIs keys are encrypted. APIs encryption keys are generated by the application code, prohibiting any reuse and performing regular rotation. Access is limited on a need to know basis through the implementation of a mandatory justification request. Such access and all actions derived therefrom are logged. The access authorization is temporary and is subject to an automatic logout at the end of the same business day.

  Toutes les clés des API de la plateforme Pennylane sont chiffrées. Les clés de chiffrement des APIs sont générées par le code de l'application, interdisant toute réutilisation et effectuant une rotation régulière. L'accès est limité au besoin d'en savoir par la mise en place d'une demande de justification obligatoire. Ces accès et toutes les actions qui en découlent sont enregistrés. L'autorisation d'accès est temporaire et fait l'objet d'une déconnexion automatique à la fin du même jour.

- Developers are technically forced to run local checks, to verify if the code being updated/added complies with the rules in terms of security, performance and coverage. The checks contain global best practices in the industry, as well as custom business checks to detect dangerous behavior for specific vulnerability classes. Furthermore, an integrity check of the remote packages installed and a disk encryption check of the developer's workstation are also part of the security hooks.

  Les développeurs sont techniquement obligés d'exécuter des contrôles locaux, pour vérifier si le code mis à jour/ajouté est conforme aux règles en termes de sécurité, de performance et de couverture. Ces vérifications contiennent les meilleures pratiques du secteur, ainsi que des vérifications métier sur-mesure visant à détecter les comportements dangereux pour des classes de vulnérabilités spécifiques. En outre, un contrôle d'intégrité des paquets installés à distance et un contrôle du chiffrement du disque du poste de travail du développeur font également partie des contrôles de sécurité.

- Pennylane runs, through continuous integration of any new code or modified code, extensive static analysis to detect and block any unsafe coding style or use of dangerous methods, and requesting when necessary the mandatory review of an Application Security engineer.

  Pennylane effectue, par le biais de l'intégration continue de tout nouveau code ou code modifié, une analyse statique approfondie afin de détecter et de bloquer tout style de codage dangereux ou toute utilisation de méthodes dangereuses, et demande si nécessaire la révision obligatoire d'un ingénieur de sécurité.

- A formal development procedure is available for developers, requesting pull requests to be systematic, reviewed by peers, passing continuous integration checks and be run on dedicated staging environments, logically separated from the production environment.

  Les développeurs disposent d'une procédure formelle de développement formelle, qui prévoit que les demandes de déploiement de code soient systématiques, examinées par des pairs, qu'elles passent les contrôles d'intégration continue et qu'elles soient exécutées sur des environnements dédiés, logiquement séparés de l'environnement de production.

- Pennylane's application external dependencies are automatically updated by a dedicated program and regularly audited by a dedicated Application Security team.

  Les dépendances externes des applications Pennylane sont automatiquement mises à jour par un programme dédié et régulièrement audité par une équipe dédiée à la sécurité des applications.

- Pennylane's application has been certified CASA Tier 2 (Cloud Application Security Assessment) by an external independent auditor of the App Defense Alliance. This certification is built upon the industry-recognized standards of the OWASP's Application Security Verification Standard (ASVS) to provide a consistent set of requirements to harden security of cloud applications.

  L'application Pennylane a été certifiée CASA Tier 2 par un auditeur externe indépendant de l'App Defense Alliance. CASA s'appuie sur la norme ASVS (Application Security Verification Standard) pour les applications OWASP, reconnue par l'industrie, afin de fournir un ensemble cohérent d'exigences pour renforcer la sécurité des applications.

AI features

- Data is hosted in the European Union by certified providers with a contractual commitment that data is never used for model training.

  Les données sont hébergées en Union européenne par des fournisseurs certifiés, avec l'engagement contractuel que les données ne sont jamais utilisées pour l'entraînement des modèles.

- The infrastructure includes strict security measures including access control, data isolation between users, and data encryption. Penetration tests are performed twice a year.

  L'infrastructure comprend des mesures de sécurité strictes incluant le contrôle des accès, l'isolation des données entre utilisateurs, et le chiffrement des données. Des tests de pénétration sont effectués deux fois par an.

- The architecture consists of four levels: Pennylane frontend for display, backend for security and authentication, ML Engine for AI logic, and hosting providers for request processing.

  L'architecture se compose en quatre niveaux : le frontend Pennylane pour l'affichage, le backend pour la sécurité et l'authentification, le ML Engine pour la logique IA, et les hébergeurs pour le traitement des requêtes.

- The features are developed in compliance with our internal security policies (ISO 27001 certified), GDPR and AI Act, with a focus on transparency and documentation. More details in our "Security and Data Management within AI features" whitepaper, available on https://www.pennylane.com/fr/securite.

  Les fonctionnalités sont développées en conformité avec nos politiques de sécurité internes (certifiées ISO 27001), le RGPD et l'IA Act, avec un focus sur la transparence et la documentation. Plus d'informations disponible dans notre livret blanc "Sécurité et gestion des données au sein des fonctionnalités IA", disponible sur https://www.pennylane.com/fr/securite.

Availability, Incidents, Backups

- All data are continually replicated in real time on secondary AWS servers distant from the primary, with an automatic failover system allowing to switch in seconds to a new server in case of failure.

  Toutes les données sont continuellement répliquées en temps réel sur des serveurs AWS secondaires distants du primaire, avec un système automatique permettant de basculer en quelques secondes sur un nouveau serveur en cas de panne.

- All data are continually backed-up, allowing to restore at any point in time at least 5 minutes ago. The recovery time of a backup is 1 hour. The full recovery process is checked twice a year for performance and improvements.

  Toutes les données sont sauvegardées en permanence, ce qui permet de restaurer à tout moment des données datant d'au moins 5 minutes. Le temps de récupération d'une sauvegarde est de 1 heure. Le processus de récupération complète est vérifié deux fois par an pour en améliorer les performances.

- Pennylane maintains a set of documented Incident Management plans with clear ownership and procedures, according to the incident severity and impact, to ensure its employees and systems performance for business continuity:

  Pennylane maintient un ensemble de plans de gestion des incidents documentés, avec des responsables et des procédures claires, en fonction de la gravité et de l'impact de l'incident, afin de garantir la performance de ses employés et de ses systèmes pour la continuité des activités :

  - Information Security Incident and Fraud Management Procedure
  - Data Breach Response Procedure
  - Incident Response Plan (PCA / PRA)

- Pennylane carries out an annual business continuity exercise to assess the company's ability to organize its response to critical incidents affecting infrastructure and services, in accordance with internal policies and controls organizing incident response and business continuity as part of ISO 27001 and DORA compliance. An executive summary of the last exercise report is available on demand.

  Pennylane réalise annuellement un exercice de crise cyber pour évaluer sa capacité à organiser une réponse organisationnelle face à des incidents critiques affectant l'infrastructure et les services, conformément aux politiques et contrôles internes organisant la réponse à incident et la continuité d'activité dans le cadre de la conformité à l'ISO 27001 et DORA. Un résumé du dernier rapport d'exercice en date est disponible sur demande.

- Pennylane does not depend on any physical premises for the continuity of its services, relying entirely on industry-leading service providers for servers, hosting and infrastructure management, services offering industry-leading scalability, data availability, security, performance, and documented business continuity plans.

  Pennylane ne dépend d'aucun local physique pour la continuité de ses services, s'appuyant entièrement sur des fournisseurs de services de premier plan pour les serveurs, l'hébergement et la gestion de l'infrastructure, services offrant une extensibilité, une disponibilité des données, une sécurité et des performances de premier plan, ainsi que des plans de continuité des activités documentés.

Legal

- Pennylane values a fair and secure usage of its customer data. A dedicated team works to fulfill Pennylane obligations, especially regarding the GDPR, through strict policies and internal regulations:

  Pennylane valorise un usage équitable et sécurisé des données de ses clients. Une équipe dédiée travaille à remplir les obligations de Pennylane, notamment en ce qui concerne le RGPD, grâce à des politiques strictes et des règlements internes :

  - Data Retention Policy
  - Data Subject Rights Procedure
  - Data Breach Response Procedure
  - Employee Privacy Policy

- Pennylane has documented its policy concerning Users' rights in a Data Subject Rights Procedure, especially regarding data access, rectification, erasure, restriction, portability, legacy, objection.

  Pennylane a documenté sa politique concernant les droits des utilisateurs dans une *Data Subject Rights Procedure*, notamment en matière d'accès aux données, de rectification, d'effacement, de restriction, de portabilité, de legs, d'opposition.

- Pennylane legal department is responsible for the risks and global compliance overview, for all operations and scopes. This responsibility is extended to all internal auditing processes including on suppliers, on finance, fraud, applicable legislation, contracts, etc.

  Le département juridique de Pennylane est responsable des risques et de la conformité globale, pour toutes les opérations et tous les domaines. Cette responsabilité s'étend à tous les processus d'audit interne, notamment sur les fournisseurs, les finances, la fraude, la législation applicable, les contrats, etc.

Audit

- Pennylane organizes continual and regular audits of its Information Systems, automatically as by internal and independent professionals, at least once a year, as part of the ISO 27001 annual certification process.

  Pennylane organise des audits continus et réguliers de ses Systèmes d'Information, automatiquement comme par des professionnels internes et indépendants, au moins une fois par an, dans le cadre du processus annuel de certification ISO 27001.

- Pennylane deploys automated technologies to offer internally an audit trails over its infrastructure and application, allowing ad hoc changes tracking, bugs and unavailability monitoring for continual improvement of the software layer.

  Pennylane déploie des technologies automatisées pour offrir en interne une piste d'audit sur son infrastructure et ses applications, permettant le suivi des changements, la surveillance des bugs et des indisponibilités pour une amélioration continue de la couche logicielle.

- The Pennylane application security is regularly tested by internal and independent security researchers against vulnerabilities and bugs, at least twice a year. An executive summary of the last to date audit report is available on demand.

  La sécurité de l'application Pennylane est régulièrement testée par des chercheurs en sécurité internes et indépendants contre les vulnérabilités et les bugs, au moins deux fois par an. Un résumé du dernier rapport d'audit en date est disponible sur demande.

Contact

Guillaume Gohin - Head of Information and Security

guillaume.gohin@pennylane.com

security@pennylane.com