Flanks

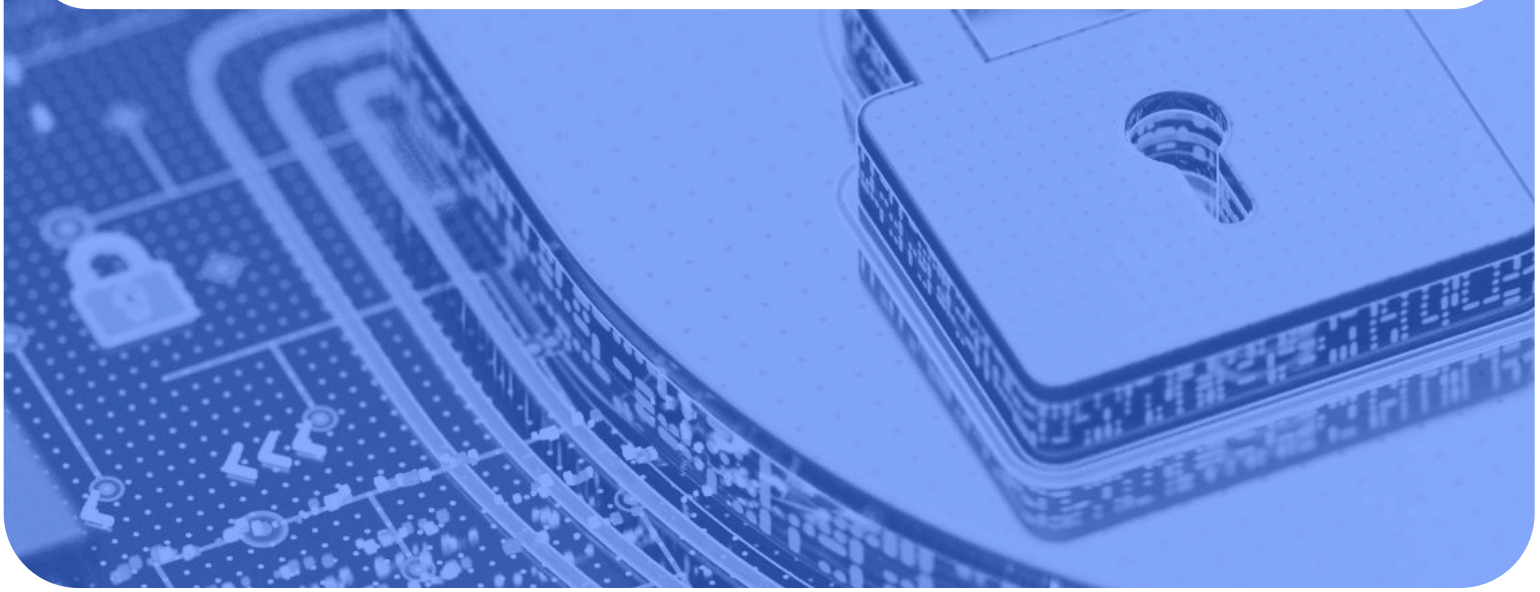
flanks.io

Livre blanc

La sécurité: au cœur des préoccupations de Flanks

avec Sergi Lao

Chief Information Security Officer et Co-fondateur



Le Contexte de l'Open Banking

Depuis 2018, l'Open Banking s'est développé dans de nombreux pays à travers le monde pour s'imposer désormais comme un dispositif incontournable pour les acteurs du secteur bancaire. Les clients veulent pouvoir disposer d'une vue consolidée unique de leur patrimoine.

Même si la réglementation européenne PSD2 cible uniquement les comptes courants, la consolidation des comptes d'investissement est devenue un aspect primordial. En Amérique latine et au Moyen-Orient, les gouvernements n'ont, à ce jour, adopté aucune réglementation en la matière.

L'adoption de l'Open Banking dans la gestion de patrimoine est un phénomène récent, mais en pleine expansion. Il reste toutefois à établir une norme opérationnelle mondiale pour le partage des données financières de nos clients. **À ce jour, une méthode globale, unifiée et sûre de partage des données financières demeure un enjeu majeur qu'il convient de prendre en considération.**

Assurer la confidentialité, l'intégrité et la disponibilité des données est devenue une priorité absolue pour Flanks, en sa qualité d'AISP (Account Information Service Provider).
Cela implique de veiller à ce que nos clients aient la certitude que leurs informations sont en sécurité.

Flanks veille à ce que la confidentialité, l'intégrité et la disponibilité constituent pour ses équipes des priorités de chaque instant.

Nous avons donc **demandé au principal expert de Flanks en matière de cybersécurité, Sergi Lao, directeur de la sécurité de l'information et cofondateur de la société, de nous accorder un entretien concernant cette problématique.**

Ce livre blanc vise à clarifier tout doute ou toute question que vous pourriez avoir sur les normes de sécurité de Flanks™, les processus à l'origine de notre collecte de données, et tout ce qui s'y rapporte.

Sergi Lao
CISO et Co-fondateur

1 Pourquoi la sécurité est-elle si importante aujourd'hui ?

De nos jours la cybersécurité revêt une importance cruciale dans tous les secteurs, mais c'est particulièrement critique dans les domaines qui traitent des données sensibles, comme la santé et la finance.

En outre, sécurité et expérience utilisateur doivent coexister sans compromis, ce qui constitue un véritable défi. Les entreprises de ces secteurs ont le devoir de garantir le respect de la vie privée, la confidentialité et l'intégrité des données. Les services financiers sont soumis à des réglementations très strictes en termes de sécurité, de qualité et de transparence.

2 Quelles sont les mesures prises par Flanks en termes de sécurité ?

Nous avons mis en place des mesures de protection qui permettent de conserver les données en toute sécurité dans ses trois états : en transit, au repos (inactives) et en cours d'utilisation. Nous nous appuyons sur la sécurité physique et sur les certifications en matière de qualité et de sécurité de la plateforme Google Cloud.

Toutes les communications, qu'elles soient externes ou internes, respectent des normes de chiffrement des données. Ces méthodes (connues sous le nom de RSA et AES -256) ne sont pas personnalisées, mais sont au nombre des normes reconnues par le marché comme étant sûres et éprouvées.

Flanks est une **société certifiée, SOC3, SOC2 Type II,** ce qui démontre notre engagement en faveur d'un contrôle rigoureux du traitement et de la sécurité des données.

Nous sommes également réglementés en tant que fournisseurs de services d'information sur les comptes (AISP). À ce titre, la Banque d'Espagne valide nos procédures et processus. En outre, nous sommes soumis à des audits annuels réalisés par des sociétés externes telles que EY.

3 Qu'est-ce qu'un fournisseur de services d'information sur les comptes (AISP) ?

Un fournisseur de services d'information sur les comptes est une société autorisée à recueillir et regrouper les informations relatives aux différents comptes bancaires détenus par un client auprès des banques et autres institutions financières.

L'AISP, qui est un acteur clé de l'environnement actuel de l'Open Banking, propose un service de base nécessitant un processus rigoureux de traitement des demandes. La licence AISP de la Banque d'Espagne nous confère l'autorisation officielle requise pour accéder aux données financières et les traiter en toute sécurité, preuve s'il en est de notre crédibilité et de notre fiabilité dans le secteur financier.

Le statut d'AISP permet à une société financière telle que Flanks de compiler des données provenant de plusieurs comptes bancaires. L'AISP explicite également à l'utilisateur final les données qui seront consultées, pendant combien de temps et qui y aura accès. Le parcours concernant le consentement numérique constitue la base du traitement des données par les AISP conformément au **RGPD.**

De plus, en tant qu'AISP, nous respectons des normes et mettons en place des méthodologies de sécurité que nous pouvons appliquer aux comptes courants et autres produits financiers. De cette manière, nous garantissons que l'intégralité des **processus est auditée, sécurisée et contrôlée.**

4 Où les données sont-elles stockées ?

Flanks se concentre sur l'intégration de données financières issues de n'importe quel système. Nous offrons une flexibilité optimale quant au stockage des informations, y compris la possibilité de les sauvegarder selon différents modèles et dans différents lieux, partout dans le monde. Nous pouvons également limiter ou élargir la portée des données sauvegardées afin de garantir une confidentialité maximale, conformément au principe de minimisation du RGPD.

Notre solution propose deux modèles de stockage de données: **sur site ou dans le cloud (Software as a Service - SaaS).** Dans les deux cas, les données et les identifiants sont obtenus avec le consentement du client. Dans le premier cas, les données extraites et les identifiants sont hébergés dans l'environnement informatique du client. Il incombe à l'équipe informatique de ce dernier de gérer leur sécurité et le bon fonctionnement de la solution proprement dite. Le client peut solliciter l'équipe Flanks à tout moment en cas de doute. Si vous choisissez la seconde option, vos données et identifiants seront stockés en Europe, aux Pays-Bas plus précisément. Flanks sera alors responsable de l'hébergement, de la maintenance et de la sécurité. Nous gérons et sécurisons également vos identifiants, et les données et identifiants seront cryptés et dissociés des clés de chiffrement.

5 Quel est l'impact dans la pratique pour nous, clients?

En tant que société réglementée, Flanks effectue des contrôles complets sur le consentement de chaque investisseur, conseiller et sur leurs accès respectifs à la banque en ligne. De même, toutes les informations relatives à leurs investissements passés et présents sont chiffrées de bout en bout. S'agissant de la confidentialité des données, Flanks agit en qualité de sous-traitant au sens du RGPD. Ce qui signifie que nous ne communiquons aucune donnée à des tiers non autorisés. Flanks se conforme au RGPD et agit au nom du propriétaire des identifiants, qui donne son consentement à la collecte des données extraites et à leur partage avec notre client. Les identifiants sont transmis directement à Flanks, conformément aux normes de sécurité les plus élevées et reconnues, et le client se voit octroyer un identifiant au titre de ces informations. Enfin, l'utilisateur peut demander, à tout moment, à Flanks la **suppression des identifiants à Flanks, qui seront alors entièrement éliminés de nos bases de données.**

6 Comment accédez-vous aux données patrimoniales des clients?

Flanks propose plusieurs moyens d'accès aux données financières des clients, en fonction de leurs préférences et des capacités des institutions financières concernées.

Pour les institutions qui prennent en charge l'accès structuré aux données, nous utilisons une procuration (PoA), une méthode sécurisée et évolutive qui permet la récupération automatisée des données :

Identifiants Flanks: l'institution financière octroie à Flanks une procuration et crée à son intention un accès en ligne dédié, en lecture seule.

Nous pouvons ainsi agréger les données financières de manière indépendante sans saisir les identifiants fournis par le client, tout en garantissant une récupération sécurisée et transparente des données.

Data Feeds: cette méthode, qui nécessite également une PoA, instaure un échange de données direct et structuré entre Flanks et l'institution financière. Plutôt que de s'appuyer sur un accès au moyen via une procédure de connexion, l'institution fournit en toute sécurité des fichiers de données financières selon un format standardisé. Cette approche améliore la précision de l'automatisation et minimise l'interaction avec le client. Bien que la disponibilité des Data Feeds dépende des capacités de chaque institution, cette méthode constitue le moyen le plus efficace et le plus évolutif d'agréger les données de patrimoine.

7 Existe-t-il une méthode d'accès aux données via une PoA qui soit meilleure que les autres ?

Toutes les méthodes garantissent un accès sécurisé et fiable aux données, mais les **Data Feeds** constituent cependant l'option la plus efficace et la plus évolutive. Ils minimisent l'interaction avec le client en automatisant la récupération des données, renforcent la sécurité grâce à des échanges structurés approuvés par l'institution et offrent une expérience utilisateur d'une grande fluidité par rapport à l'accès au moyen d'identifiants.

De plus, les institutions financières privilégient souvent les Data Feeds, car ils rationalisent la gestion des données et renforcent la sécurité, l'efficacité et l'évolutivité de l'agrégation des données financières. Pour résumer, toutes ces solutions sont efficaces, mais les Data Feeds offrent le meilleur équilibre entre la sécurité, la commodité et l'efficacité opérationnelle.

8 Quelle est la procédure pour les clients souhaitant opter pour une méthode autre que la PoA ?

Les clients peuvent également utiliser leurs propres identifiants ; dans certains cas, ce choix implique de mettre en **place une authentification forte du client (SCA) (également connue sous le nom de 2FA)** pour se connecter aux institutions financières en toute sécurité. Contrairement à la PoA, qui nécessite une seule interaction avec le client en tout début de processus, l´identifiant client requiert des autorisations périodiques de sa part.kms

Flanks ne déclenche le SCA que lorsque l'utilisateur est activement présent, évitant ainsi les demandes inutiles et réduisant le risque de mauvaises habitudes, comme l'approbation de notifications inconnues. Nous prenons en charge plusieurs méthodes d'authentification, notamment les codes SMS, les appels téléphoniques, les applications d'authentification, la biométrie, les clés de sécurité et les codes QR et, ce, toujours dans le respect des politiques de sécurité de chaque dépositaire.

9 De quelle façon Flanks garantit-elle que les identifiants de mon client sont sécurisés s'il utilise les informations d'identification qui lui sont propres?

Flanks stocke les accès par le biais d'un processus de double chiffrement en utilisant le service KMS de Google Cloud. Les identifiants ne sont conservés qu'avec le consentement de l'utilisateur, qui accepte que Flanks transfère les données extraites au client final (conseiller financier ou application proposant la consultation des investissements). Chaque opération faisant intervenir les identifiants gérée par Flanks est strictement surveillée, enregistrée et s'effectue, par défaut, en lecture seule. **Les codes SCA ne sont stockés nulle part.**

10 Comment assurez-vous l'accès en lecture seule à l'interface?

Pour des raisons réglementaires, les entités financières imposent l'utilisation d'un protocole SCA pour effectuer toute opération ayant un impact direct et irréversible sur leur situation financière, comme un virement bancaire, l'achat d'actions ou le transfert d'un fonds d'investissement. L'accès accordé à **Flanks ne lui permet donc pas d'apporter de modification irréversible à un compte.** De même, la société est réglementée et auditée afin de renforcer la confiance que nos utilisateurs nous accordent à Flanks. Nous conservons la traçabilité de la date et du type de données extraites dans le cadre de toutes nos agrégations.

11 Un client ne viole-t-il pas les conditions générales de la banque dépositaire s'il transmet ses identifiants à un tiers?

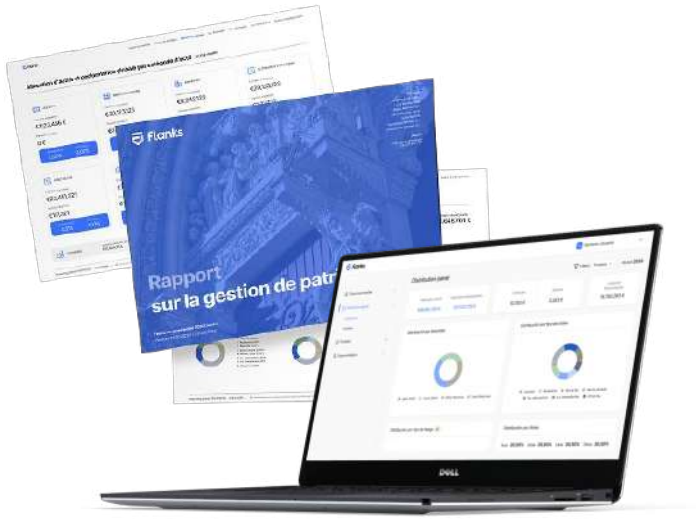
C'est impossible, car le RGPD prévaut systématiquement sur n'importe quelle politique interne. Cela signifie que, bien qu'une entité financière puisse disposer de politiques ou des conditions générales allant à son encontre, **l'utilisateur a le droit de partager des données avec une entité tierce.**

Flanks se conforme aux réglementations **PSD2 et RGPD** et dispose de différents rapports d'avis juridiques contraignants qui valident l'utilisation de l'outil mis à votre disposition. Flanks simule le comportement d'un navigateur web et limite l'utilisation de la bande passante afin d'éviter toute perturbation du site web de l'institution financière. N'hésitez pas à nous contacter si vous avez des doutes ou des questions à ce sujet.

12 Comment puis-je commencer à bénéficier des Flanks?

Vous pouvez nous contacter via la page Contact de notre site web. En cas de doute, n'hésitez pas à planifier un premier entretien avec notre équipe de vente que ce soit en espagnol, anglais, français ou portugais.

Nous sommes là pour vous aider et répondre à toutes les questions que vous vous posez quant à votre transformation digitale.



Contactez-nous

Nos experts en patrimoine sont à votre écoute ! Vous souhaitez en savoir plus ? Contactez-nous !

Flanks

Wealth, easily managed

Et si nous en discutions?

Flanks.io