

Fiche sécurité et protection des données

Produit : Noa by MoveBreak
Éditeur : MOVELYTICS, SASU — SIREN 948 127 493
Siège : CHEZ ESTIA Entreprendre, 97 allée Théodore Monod, 64210 Bidart, France
Contact protection des données : fabrice@move.lytics.fr
Version : 1.0 — 7 septembre 2026
Périmètre : application Microsoft Teams uniquement (bot 1:1 + onglets Config et Bibliothèque)

Cette fiche ouvre le dialogue avec une DSI, un RSSI ou un DPO. Elle décrit le service **tel qu’il est en production**, pas un SMSI cible. Les éléments absents sont listés en section 10. **Si vous avez des exigences de pentest, d’ISO, de certification ou d’hébergement (PaaS imposé, instance dédiée) pour un prestataire comme nous, transmettez-les en entier dès ce premier échange** (voir § 2.1 et § 10).

Documents associés : modèle de DPA (article 28 RGPD), note DORA de premier échange, annexe technique.

Pages publiques : [politique de confidentialité](#) · [conditions](#) · [listing Microsoft](#)

1. Le service, en une page

Noa envoie aux collaborateurs des rappels de courtes pauses bien-être dans Microsoft Teams et propose des contenus (mouvement, micro-learning, bibliothèque vidéo). Le déploiement est réalisé par la **DSI** du client, à l’échelle du tenant ou d’un sous-ensemble d’utilisateurs. **Aucun salarié n’installe l’application ni ne crée de compte** : le compte technique est provisionné lors de l’installation du bot dans l’environnement Microsoft 365 de l’organisation.

L’usage se fait dans une conversation 1:1 avec le bot, plus deux onglets personnels Teams (**Config** et **Bibliothèque**). Noa n’est **pas** un agent Copilot / LLM. Il n’analyse pas les autres conversations, canaux, réunions, e-mails, fichiers, calendriers ou contacts de l’organisation.

L’application Teams est **gratuite avec des limites d’usage**. Les offres payantes s’adressent aux organisations et sont **facturées en direct** (contrat / licence entreprise). Il n’y a pas d’abonnement personnel ni de paiement carte dans Teams.

Effectif éditeur : **startup de trois personnes**. Pas de sous-traitance de développement tierce pour ce backend.

2. Architecture et hébergement

Élément	Choix retenu
Nature	Application SaaS, backend PaaS (pas d’IaaS géré par MOVELYTICS)
Hébergeur applicatif	Heroku (Salesforce)
Base de données	PostgreSQL managé Heroku
Région des données applicatives	Union européenne, Irlande (eu-west-1)
Runtime	Node.js, API HTTP Express
Canal Teams	Microsoft Bot Framework / Azure Bot Service
TLS	Terminaison chez l’hébergeur (TLS 1.2+) ; HSTS 180 jours sur le backend

MOVELYTICS ne gère pas d’hyperviseurs, de réseau physique ni de disques **dans l’offre actuelle**. Une part importante de la sécurité d’infrastructure (patches OS, isolation, sauvegardes Postgres du PaaS) relève du **contrat Heroku / Salesforce**. MOVELYTICS reste responsable de l’application, des secrets, des habilitations et du code.

2.1 Ouverture : autre PaaS ou instance dédiée chez le client

L'hébergement Heroku est le **choix actuel**, pas un engagement irréversible.

Si la politique du client l'exige, MOVELYTICS est **ouverte à discuter**, dans un **cadre écrit** (avenant d'hébergement : périmètre, responsabilités, accès, isolation, délai, coût) :

1. **Changer de PaaS** pour une plateforme que le client accepte (cloud / PaaS UE ou offre déjà homologuée chez lui), MOVELYTICS continuant d'exploiter l'application ; ou
2. **Une instance dédiée** du backend et de la base, sur des **serveurs et une base de données appartenant au client** (tenant cloud du client, ou infrastructure qu'il désigne), distincte du SaaS mutualisé.

Ce n'est **pas** l'offre par défaut, **pas** un livrable immédiat, et **pas** un dépôt de code « à vous de faire tourner » sans modèle d'exploitation. Le canal **Microsoft Teams / Bot Service** reste nécessaire au produit (ce n'est pas substituable par un PaaS). Toute bascule se fait après cadrage : qui administre, qui a les secrets, qui patch, qui sauvegarde, comment MOVELYTICS accède au support, comment les Données restent isolées des autres clients.

Les contraintes d'hébergement (PaaS interdit, cloud interne obligatoire, région, labels) doivent être **transmises dès le premier échange**, comme les exigences pentest / certification.

Schéma de flux (simplifié) :

```
Collaborateur → Microsoft Teams
|
├─ messages bot — JWT Azure Bot Service → POST /api/messages → Heroku / Postgres
└─ onglets Config / Bibliothèque — HTTPS → même backend (contexte Teams userId)
```

Les contenus vidéo de la Bibliothèque sont lus dans un lecteur **YouTube** ou **Vimeo** lorsque l'utilisateur lance une vidéo. L'e-mail d'invitation calendrier (**Move Invitation**) passe par **Brevo** (SMTP) uniquement si la fonctionnalité est utilisée.

3. Permissions Microsoft Teams — ce que Noa peut et ne peut pas

Point	Situation
Microsoft Graph	Aucun appel. Pas de lecture d'annuaire, mail, fichiers, calendrier, chat d'équipe.
Resource-specific consent (RSC)	Liste vide dans le manifeste.
SSO d'onglet (<code>getAuthToken</code> / <code>webApplicationInfo</code>)	Non activé. La vérification éditeur Microsoft (domaine personnalisé + MPN) est en cours ; l'activer trop tôt casserait le consentement.
Authentification du bot	Jeton JWT émis par Azure Bot Service, validé sur <code>POST /api/messages</code> .
Onglets	Identification par le contexte Teams (<code>userId</code> / tenant). Pas de mot de passe Noa.
Portée du bot	Conversation personnelle (1:1). Pas d'appels, pas de visio, pas de fichiers.
Publication	Application listée sur le marketplace Microsoft (identifiant listing WA200008766). Ce n'est pas une certification Microsoft 365.
Vérification éditeur	En cours (les domaines <code>onmicrosoft.com</code> ne sont pas acceptés comme domaine d'éditeur).

En pratique : Noa ne voit que ce que l'utilisateur échange **avec Noa**, plus le profil Teams nécessaire au bot (nom, e-mail affichés, identifiants techniques).

Identifiants techniques utiles au client :

- ID application Teams (manifeste) : `2a175964-2610-4c07-af50-d6a5d691c924`
- ID bot / application Entra (bot) : `8bf8b0c0-4eb2-44a0-92a2-aba236e64e52`
- Hôte backend : `move-break-microsoft-teams-app-04b9b0a5156b.herokuapp.com`

4. Données personnelles

4.1 Stockées (Postgres)

- Identifiants : `userId` Entra, `tenantId`, e-mail et nom tels que transmis par Teams (`TeamsInfo`).
- Référence de conversation Teams (nécessaire aux **rappels proactifs**) — **exclue** de l'export JSON utilisateur.
- Préférences : horaires et jours de rappel, fuseau, zones corporelles, matériel déclaré, micro-learning, onboarding, invitations calendrier.
- Usage : historique de pauses, sessions / favoris Bibliothèque, scores d'usage (Move Score).
- Licences entreprise du tenant (statut, dates) — données de contrat, pas de carte bancaire.
- Trace minimale après effacement : identifiant, tenant, date, motif (`user_request` ou `tenant_churn`), pour afficher le bon message et empêcher une recréation silencieuse.

4.2 Qui transitent sans être « le métier »

- Jeton Bot Framework (validé, non stocké comme secret utilisateur).
- Adresse IP (limitation de débit, sécurité).
- Contenu des cartes et messages **dans** la conversation Noa, traité pour le service.

4.3 Non collectées / non recherchées

Graph, e-mails Outlook, autres chats Teams, fichiers M365, calendrier et contacts via API, données de paiement dans Teams, **humeur (mood)** — la collecte est arrêtée, les écritures sont ignorées.

4.4 Données de santé (article 9 RGPD) — point critique

Noa **n'est pas** un dispositif médical. Il ne collecte pas de diagnostics, certificats, comptes rendus ou données cliniques.

Les **zones corporelles** (dos, nuque, etc.) sont des **préférences fonctionnelles** pour adapter les exercices. Elles ne constituent pas, dans le dessin du produit, une collecte intentionnelle de données de santé. Le client ne doit pas utiliser Noa pour y consigner des informations médicales.

Si une DSI classe malgré tout ces préférences en article 9, le traitement nécessiterait un cadre supplémentaire (base, AIPD, instructions) **non couvert** par le produit actuel : à discuter avant tout déploiement dans ce cas.

4.5 Ce que l'employeur voit

Le tableau de bord **tenant** (réfèrent client `is_admin`) expose des **indicateurs agrégés** : volumes d'utilisateurs, taux d'activité, minutes de pause, zones au niveau collectif, score d'engagement. **Pas** l'historique nominatif d'un salarié, **pas** ses préférences personnelles, **pas** ses réponses individuelles.

Noa n'est pas un outil de surveillance individualisée.

Les équipes MOVELYTICS (trois personnes, comptes `is_movebreak_admin`) peuvent accéder aux données pour le **support et l'exploitation**, avec un journal d'accès interne. Ce n'est pas le même écran que le tableau de bord client.

5. Droits des personnes et conservation

Mécanisme	Règle réelle
Accès / portabilité	Export JSON depuis Config (« Mes données »), ou e-mail <code>fabrice@move.lytics.fr</code> (délai 30 jours)
Effacement individuel	Même écran, confirmation explicite, même si l'entreprise est encore cliente
Recréation	Uniquement après un effacement à la demande de l'utilisateur ; pas après une purge de fin de contrat
Inactivité d'un salarié chez un client	Pas de purge. Tant que l'organisation a une licence entreprise active ou en essai, le compte reste disponible.

Fin de contrat	Délai de grâce 90 jours après la fin de la dernière licence entreprise, puis suppression des comptes du tenant
Désactivation des rappels (<code>stop</code> / Config)	Arrête les notifications ; n'efface pas les données

L'export ne contient pas la référence technique de conversation. Après effacement, les lignes d'historique de pauses sont **détachées** de l'identifiant (conservées pour des stats agrégées du tenant).

6. Mesures de sécurité (ce qui existe)

- Hébergement PaaS + Postgres managé, région UE.
- HTTPS / TLS ; **HSTS** 180 jours ; `X-Content-Type-Options: nosniff` ; `Referrer-Policy: no-referrer` .
- **CSP** `frame-ancestors` limité aux origines Teams / Office (onglets iframés).
- Limitation de débit sur les API (hors canal Bot Framework, pour ne pas casser les messages Teams).
- Requêtes SQL **paramétrées**.
- Logs bot / rappels : **pas d'e-mail ni de nom** ; messages non reconnus stockés en **empreinte (hash) + longueur**, sans le texte libre.
- Pas de Graph, RSC vide, moindre privilège côté Microsoft 365.
- Secrets applicatifs dans la configuration Heroku (non versionnés dans le dépôt public de ce dossier).
- Sauvegardes et continuité : celles du **Postgres Heroku** (plan de l'hébergeur), pas un PRA documenté MOVELYTICS autonome.

7. Sous-traitants techniques

Prestataire	Rôle	Données / condition
Microsoft	Teams, Bot Service, Entra	Transport des messages, identité Teams
Heroku / Salesforce	PaaS + PostgreSQL	Backend et base par défaut — substituable (voir § 2.1)
Brevo	E-mail transactionnel	Uniquement si Move Invitation est utilisée
YouTube / Vimeo	Lecteur vidéo	Uniquement si l'utilisateur lance une vidéo

Pas de Stripe dans l'app Teams. Pas de Notion en production (synchronisation désactivée).

Des accès de support de ces prestataires **peuvent** impliquer un transfert hors EEE ; les mécanismes sont ceux de leurs DPA / CCT (à joindre sur demande).

8. Organisation

Sujet	Situation
Effectif	3 personnes
Référent données / sécurité	Fabrice, <code>fabrice@move.lytics.fr</code> (pas de DPO externe nommé dans ce document)
Sous-traitance de développement	Non, pour ce backend
Notification de violation	Information du client sans délai injustifié , et au plus tard dans les délais de l'article 33 RGPD côté responsable de traitement (voir DPA)
Certification / pentest	Aucun passé à ce jour. Options explorées ; exigences client à transmettre dès le départ (section 10)

9. DORA — en deux phrases

Noa est un **outil de bien-être dans Teams**, pas un système de paiement, de core banking ou de messagerie métier critique. La qualification « prestataire TIC critique / important » relève du **client**. Notre position détaillée (clauses tenables vs non tenables aujourd'hui) est dans la note DORA jointe.

10. Ce que nous n'avons pas encore mis en place

Cette section est volontaire. Une DSI bancaire doit pouvoir s'en servir.

À ce jour, aucun pentest ni aucune certification n'a été passé (ISO 27001, SOC 2, certification Microsoft 365 App Certification, ou équivalent). Nous ne les inventons pas. Nous **explorons les options** (prestataires, périmètre, coût, charge pour une équipe de trois personnes).

10.1 Ce que nous vous demandons dès ce premier échange

Si votre organisation impose à une **solution tierce** comme Noa un test d'intrusion, une certification, un référentiel de sécurité, des clauses DORA particulières, un droit d'audit spécifique, un questionnaire type, un délai de correction des vulnérabilités, **un PaaS imposé ou une instance sur votre infrastructure**, etc. : **transmettez-nous l'ensemble de ces exigences maintenant**, pas une fois le pilote lancé.

Cela nous permet, avant d'aller plus loin :

1. d'engager les démarches **si nous pouvons nous les permettre** (budget, délai, capacité) ; ou
2. de vous **prévenir tout de suite** que telle exigence ne sera pas tenable — plutôt qu'un blocage en fin de processus.

Sans le référentiel complet, nous ne pouvons ni confirmer une mise en conformité, ni annoncer un délai réaliste.

Contact : fabrice@moveitytics.fr.

10.2 État des lieux

Élément	État	Horizon
Tests d'intrusion (boîte noire / grise / blanche)	Aucun passé	Exploré ; calendrier seulement si une exigence client (ou une décision interne) le rend nécessaire et finançable
ISO 27001 / SOC 2	Aucune obtenue	Idem : pas d'engagement de date tant que l'exigence et le coût ne sont pas posés
Certification Microsoft 365 App Certification	Non obtenue, non demandée	Bloquée sans pentest annuel et sans éditeur vérifié
Vérification éditeur Microsoft (MPN + domaine DNS custom)	En cours	Préalable au SSO d'onglet
SSO Entra sur les onglets Config / Bibliothèque	Non	Après vérification éditeur
SMSI documenté, EDR flotte, scans trimestriels formalisés	Absents en tant que dispositif auditable	Processus interne progressivement, pas un livrable immédiat
DPO désigné auprès de la CNIL	Contact interne seulement	Si le volume / le risque l'exige plus tard
PRA / PCA chiffré (RTO/RPO MOVEITYTICS)	Dépendance au PaaS Heroku dans l'offre actuelle	Autre PaaS ou instance dédiée : possible par avenant (§ 2.1), pas packagé
Hébergement hors Heroku	Ouverture , pas une offre catalogue	Cadrer qui opère / accès / coût ; Teams reste obligatoire
Assurance RCP	À communiquer sur justificatif	Pièce à joindre au DPA

Ce que nous ne ferons pas pour « faire plaisir » : antedater un pentest, afficher un logo ISO, élargir Graph « au cas où », ou signer une clause que trois personnes ne peuvent pas tenir.

11. Comment un premier examen peut se conclure

Recevable pour un **pilote** ou un déploiement borné si le client accepte : PaaS UE (Heroku aujourd'hui, **autre cible discutable**), absence de Graph, agrégation RH, DPA art. 28, l'état des lieux de la section 10, **et** nous a transmis (ou confirmé l'absence de) ses exigences pentest / certification / clauses prestataires / **hébergement**.

Dès que le référentiel nous est remis, nous revenons par écrit : tenable / tenable sous conditions et délai / non tenable.
Pas de promesse de date avant cette étape.