

Accord relatif au traitement des données personnelles

Data Processing Agreement — article 28 du règlement (UE) 2016/679

Modèle destiné à un premier échange. À faire relire par un conseil avant signature. Les mentions [À COMPLÉTER] ne doivent pas être inventées.

Version : 1.0 — 7 septembre 2026

Périmètre produit : application **Noa** dans **Microsoft Teams** uniquement.

ENTRE

[À COMPLÉTER : **dénomination sociale du client**], [forme], SIREN [À COMPLÉTER], dont le siège est [À COMPLÉTER], représentée par [À COMPLÉTER],

ci-après le « **Responsable de traitement** » ou le « **Client** »,

ET

MOVELYTICS, société par actions simplifiée unipersonnelle (SASU), SIREN **948 127 493**, dont le siège social est situé CHEZ ESTIA Entreprendre, 97 allée Théodore Monod, 64210 Bidart, France, représentée par [À COMPLÉTER : **représentant**],

ci-après le « **Sous-traitant** » ou « **MOVELYTICS** »,

MoveBreak étant la **marque** sous laquelle le service Noa est proposé ; elle ne constitue pas une personne morale distincte.

ci-après ensemble les « **Parties** ».

Préambule

Le Client déploie l'application **Noa** dans Microsoft Teams au bénéfice de tout ou partie de ses collaborateurs. Les utilisateurs finaux n'installent pas l'application eux-mêmes et ne créent pas de compte distinct : le déploiement est réalisé par la DSI (ou service équivalent) du Client.

MOVELYTICS fournit le service SaaS d'exploitation de Noa (bot de conversation 1:1, onglets Config et Bibliothèque, rappels de pauses bien-être et contenus associés).

Le présent Accord constitue le contrat de sous-traitance exigé par l'**article 28 du RGPD**. Il s'applique aux traitements de données personnelles que MOVELYTICS effectue **pour le compte du Client** dans ce cadre. Il complète le contrat commercial / les conditions applicables ; en cas de conflit sur le traitement des données, **le présent Accord prévaut**.

Les traitements pour lesquels MOVELYTICS agit en **responsable de traitement** (facturation de la relation client, obligations légales propres, sécurité de sa plateforme, amélioration sur données agrégées ou anonymisées) sont décrits dans la politique de confidentialité et **ne relèvent pas** des instructions du Client, sous réserve du RGPD.

Article 1 — Définitions

Les termes « données personnelles », « traitement », « responsable de traitement », « sous-traitant », « personne concernée », « violation de données personnelles », « autorité de contrôle » ont le sens du RGPD.

Service : l'application Noa dans Microsoft Teams, telle que décrite à l'annexe I et dans l'annexe technique fournie au Client.

Données : les données personnelles traitées par MOVELYTICS pour le compte du Client au titre du Service.

Sous-traitant ultérieur : tout sous-traitant engagé par MOVELYTICS pour tout ou partie du traitement.

Article 2 — Objet et durée

2.1. MOVELYTICS s'engage à traiter les Données uniquement pour fournir le Service, conformément au présent Accord, au contrat commercial et aux **instructions documentées** du Client.

2.2. Le présent Accord entre en vigueur à la date de signature (ou, à défaut, à la date de premier déploiement du Service pour le Client) et demeure applicable tant que MOVELYTICS traite des Données pour le Client, y compris pendant le délai de grâce suivant la fin du contrat commercial (annexe I).

Article 3 — Instructions

3.1. Le Client est seul responsable de la licéité du déploiement (base juridique vis-à-vis des collaborateurs, information des personnes, éventuelle consultation des instances représentatives, politiques internes).

3.2. Les instructions du Client sont celles résultant : (a) du présent Accord et de ses annexes ; (b) de l'usage normal du Service (déploiement, paramétrage, tableau de bord agrégé) ; (c) des demandes écrites adressées à `fabrice@move.lytics.fr` (ou tout autre contact convenu).

3.3. MOVELYTICS informe immédiatement le Client si, selon elle, une instruction viole le RGPD. Elle peut alors suspendre l'exécution de cette instruction.

3.4. MOVELYTICS n'exploite pas les Données pour profiler les collaborateurs au bénéfice de tiers, ni pour de la publicité comportementale.

Article 4 — Confidentialité et personnes habilitées

4.1. MOVELYTICS s'assure que les personnes autorisées à traiter les Données (salariés, mandataires) sont tenues à une obligation de confidentialité.

4.2. L'accès interne aux Données est limité aux personnes ayant besoin d'en connaître pour l'exploitation, le support ou la sécurité du Service. À la date du présent modèle, l'effectif de MOVELYTICS est de **trois personnes**.

4.3. Un journal technique des accès d'administration interne est tenu pour les consultations concernées.

Article 5 — Sécurité

5.1. MOVELYTICS met en œuvre les mesures techniques et organisationnelles décrites à l'**annexe II**, adaptées à la nature du Service (application de bien-être dans Teams, hébergement PaaS).

5.2. Ces mesures tiennent compte de l'état des connaissances, des coûts, de la nature, de la portée et des finalités du traitement, ainsi que des risques. Elles n'équivalent **pas** à une certification ISO 27001, ni à un audit d'intrusion : **à la date du présent modèle, aucun pentest ni aucune certification (ISO 27001, SOC 2, certification Microsoft 365, ou équivalent) n'a été passé.** MOVELYTICS explore les démarches qui pourraient le devenir.

5.3. Le Client s'engage à communiquer **dès la phase précontractuelle**, et en tout état de cause avant signature, **l'ensemble** des exigences de sécurité, d'audit, de certification ou de tests d'intrusion qu'il impose aux prestataires de solutions tierces comparables au Service. MOVELYTICS indiquera alors par écrit ce qu'elle peut mettre en œuvre, sous quel délai et à quelles conditions, ou ce qu'elle ne peut pas tenir. L'absence de transmission de ces exigences ne saurait être interprétée comme un engagement de MOVELYTICS à obtenir une certification ou un pentest.

5.4. Le Client reconnaît que l'infrastructure d'hébergement (Heroku / PostgreSQL managé) et le canal Microsoft Teams relèvent en partie des mesures de ces prestataires, encadrées par leurs propres conditions et DPA.

Article 6 — Sous-traitants ultérieurs

6.1. Le Client autorise d'une manière générale le recours aux sous-traitants ultérieurs listés à l'**annexe III**.

6.2. MOVELYTICS informe le Client de tout **ajout ou remplacement** d'un sous-traitant ultérieur ayant un impact

significatif sur le traitement (nouvel hébergeur, instance dédiée chez le Client, nouvel outil d'e-mail transactionnel, rétablissement d'un prestataire de paiement dans l'application, etc.). Le Client dispose de **quinze (15) jours** pour formuler une objection écrite motivée par un risque raisonnable pour la protection des Données. À défaut, l'ajout est réputé accepté. Une objection légitime peut conduire à discuter d'une sortie du Service si aucune alternative raisonnable n'existe. Le remplacement d'Heroku ou le passage en instance dédiée suit en outre l'article 17.

6.3. MOVELYTICS impose à ses sous-traitants ultérieurs des obligations de protection au moins équivalentes, par contrat. Lorsque le prestataire est un éditeur mondial (Microsoft, Salesforce / Heroku), les DPA et clauses types de ce prestataire s'appliquent.

6.4. Les lecteurs vidéo YouTube / Vimeo ne sont sollicités que si un utilisateur lance une vidéo. Brevo n'est utilisé que si la fonctionnalité d'invitation calendrier est active.

Article 7 — Transferts hors EEE

7.1. Sauf avenant d'hébergement contraire (article 17), les données applicatives du Service sont hébergées dans l'**Union européenne** (Irlande, infrastructure Heroku / PostgreSQL, à la date du présent modèle).

7.2. Certains prestataires (notamment Microsoft, outils de support de l'hébergeur, lecteurs vidéo) peuvent impliquer un accès ou un traitement hors EEE. Dans ce cas, MOVELYTICS s'appuie sur un mécanisme reconnu (clauses contractuelles types, décision d'adéquation, ou autre instrument valable).

7.3. Le détail figure à l'annexe III. MOVELYTICS ne transfère pas les Données vers un pays tiers **pour ses propres besoins** hors de ce cadre.

Article 8 — Droits des personnes concernées

8.1. Le Client, responsable de traitement, reste l'interlocuteur principal des collaborateurs pour l'exercice de leurs droits, sans préjudice des voies de self-service ci-dessous.

8.2. MOVELYTICS met à disposition dans l'onglet Config du Service (tuile « Mes données ») :

- un **export** des données du compte (format JSON, hors référence technique de conversation Teams) ;
- un **effacement** du compte Noa, après confirmation, **y compris** si le Client est encore lié par un contrat.

8.3. MOVELYTICS assiste le Client pour les demandes reçues par ailleurs (e-mail fabrice@move.lytics.fr), dans un délai permettant au Client de respecter l'article 12 du RGPD, et au plus tard **trente (30) jours** après une demande complète, sauf complexité justifiant une prolongation dans les limites légales.

8.4. Après un effacement à la demande de la personne, celle-ci peut **recréer** volontairement son compte Noa. Après une purge liée à la fin de contrat (article 10), la recréation self-service n'est pas possible.

Article 9 — Notification des violations

9.1. MOVELYTICS notifie au Client toute violation de Données **sans délai injustifié** après en avoir eu connaissance, et en tout état de cause dans un délai permettant au Client de respecter l'article 33 du RGPD (notification à l'autorité, le cas échéant sous 72 heures).

9.2. La notification contient, dans la mesure des informations disponibles : la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables, les mesures prises ou proposées.

9.3. MOVELYTICS n'effectue pas la notification à la CNIL **à la place** du Client pour les traitements dont le Client est responsable, sauf accord contraire écrit.

Article 10 — Conservation, restitution, suppression

10.1. **Pendant le contrat.** Tant que le Client dispose d'une licence entreprise **active** ou **en essai** (`trialing`) non expirée, MOVELYTICS conserve les comptes des collaborateurs du tenant nécessaires à la mise à disposition du Service. **Aucune purge automatique pour inactivité individuelle** n'est pratiquée (un collaborateur inactif n'est pas supprimé au seul motif qu'il n'a pas cliqué pendant plusieurs mois).

10.2. **Effacement à la demande de la personne.** Voir article 8. Les historiques de pauses peuvent être conservés sous forme **détachée** de l'identifiant, pour des statistiques agrégées du Client.

10.3. **Fin du contrat.** À compter de la fin de la dernière licence entreprise applicable au tenant, MOVELYTICS observe un délai de grâce de **quatre-vingt-dix (90) jours**. Pendant ce délai, le Client peut demander par écrit :

- la **restitution** des Données dans un format usuel et raisonnablement exploitable ; ou
- la **suppression** anticipée.

À défaut d'instruction, MOVELYTICS procède à la suppression des comptes du tenant à l'issue de ce délai, hors obligation légale de conservation et hors exclusions techniques internes de l'éditeur (environnements de démonstration qui ne concernent pas le Client).

10.4. Les traces minimales d'effacement (identifiant technique, tenant, date, motif) sont conservées le temps nécessaire pour empêcher une recréation silencieuse et afficher le message adéquat, puis selon une durée raisonnable de preuve / sécurité.

10.5. Les données anonymisées ou agrégées au point de ne plus constituer des données personnelles peuvent être conservées par MOVELYTICS.

Article 11 — Assistance, AIPD, consultations

Sur demande écrite et dans la limite de ce qui est **raisonnable** eu égard à la nature du traitement et aux informations dont dispose MOVELYTICS, celle-ci assiste le Client pour :

- répondre aux demandes des personnes concernées ;
- respecter les articles 32 à 36 du RGPD (sécurité, violations, AIPD, consultation préalable).

Une analyse d'impact n'est **pas** fournie clé en main avec ce modèle : le Service n'est pas conçu comme un traitement à grande échelle de données de santé ni comme un outil de surveillance au travail. Si le Client estime qu'une AIPD est nécessaire, MOVELYTICS fournit les éléments factuels du Service (annexes).

Article 12 — Audit

12.1. MOVELYTICS met à disposition les informations nécessaires pour démontrer le respect du présent Accord, notamment la fiche sécurité, la présente annexe technique, et, sur demande, les extraits pertinents des DPA de ses sous-traitants ultérieurs.

12.2. Le Client peut faire procéder à un **audit documentaire** (questionnaires, visio, revue de politiques), **pas plus d'une fois par an** sauf violation avérée ou instruction d'une autorité, moyennant un **préavis de trente (30) jours**, pendant les jours ouvrés, sans perturber le Service.

12.3. Un audit sur site, un test d'intrusion ou un audit chez un sous-traitant ultérieur (Heroku, Microsoft) n'est **pas** un droit automatique : il fait l'objet d'un accord spécifique (périmètre, calendrier, coûts). MOVELYTICS n'a pas le pouvoir d'imposer un audit à Microsoft ou Salesforce.

12.4. Les coûts de l'audit sont à la charge du Client, sauf manquement grave de MOVELYTICS au présent Accord constaté par l'audit.

Article 13 — Données de santé et finalité

13.1. Le Service **n'a pas** pour objet de traiter des données de santé au sens de l'article 9 du RGPD (diagnostics, données cliniques, arrêts, etc.).

13.2. Les préférences de **zones corporelles** sont des paramètres fonctionnels pour adapter des exercices. Le Client s'interdit d'instruire MOVELYTICS de collecter via Noa des données médicales.

13.3. Si le Client requalifiait ces préférences en article 9, il devrait le notifier par écrit ; le Service actuel **n'est pas** configuré pour ce cadre (pas de base article 9, pas d'AIPD fournie par l'éditeur). Les Parties en discuteraient avant tout traitement en ce sens.

Article 14 — Tableau de bord du Client

MOVELYTICS ne met pas à disposition du Client, via le tableau de bord tenant du Service, l'historique nominatif d'usage d'un collaborateur, ses préférences individuelles détaillées ou ses réponses individuelles. Le Client reçoit des **indicateurs agrégés**. Le Service n'est pas un outil de contrôle individuel de l'activité.

Article 15 — Responsabilité

La responsabilité des Parties au titre du présent Accord suit le contrat commercial. À défaut de clause contraire, chaque Partie répond des dommages résultant de l'inexécution de ses obligations RGPD, dans les limites légales (notamment article 82 du RGPD). MOVELYTICS ne répond pas d'un usage du Service par le Client contraire au présent Accord (par exemple tentative de surveillance individuelle, consigne de données médicales).

[À COMPLÉTER si le contrat commercial prévoit un plafond : renvoyer à l'article X / à l'assurance RCP.]

Article 16 — Assurance

MOVELYTICS déclare **[À COMPLÉTER : détenir une assurance responsabilité civile professionnelle n° ... auprès de ..., plafond ... / ou : communiquer une attestation sur demande]**.

Article 17 — Évolution de l'hébergement

17.1. L'hébergement par défaut du backend et de la base de données est le PaaS **Heroku** (Salesforce) décrit aux annexes. Ce choix n'interdit pas aux Parties d'en convenir autrement.

17.2. Sur demande écrite du Client, MOVELYTICS examine de bonne foi, sans obligation de résultat tant qu'un avenant n'est pas signé :

- le **remplacement du PaaS** par une autre plateforme d'hébergement **acceptée par le Client** (région UE ou infrastructure déjà autorisée chez le Client), MOVELYTICS restant en principe l'exploitant applicatif ; et/ou
- une **instance dédiée** du Service (application et base de données) déployée sur des **serveurs et une base appartenant au Client** (tenant cloud du Client ou infrastructure qu'il désigne), isolée du SaaS mutualisé.

17.3. Toute bascule fait l'objet d'un **avenant d'hébergement** précisant au minimum : architecture cible, localisation, qui opère et qui patch, habilitations et secrets, sauvegardes, accès support de MOVELYTICS, isolation vis-à-vis des autres clients, calendrier, coût, et mise à jour de l'annexe III (sous-traitants). Cet avenant n'est **pas** inclus dans la signature du présent Accord seul.

17.4. Le canal **Microsoft Teams / Azure Bot Service** demeure nécessaire au Service. Il n'est pas substitué par un changement de PaaS. MOVELYTICS ne s'engage pas, par le présent article, à une mise à disposition « clé en main » sous un délai fixe, ni à un transfert du logiciel sans modèle d'exploitation.

Article 18 — Sortie, réversibilité

Outre l'article 10, MOVELYTICS coopère raisonnablement à la réversibilité : restitution convenue, suppression, confirmation écrite de purge sur demande. La réversibilité porte sur les **Données**, non sur la cession du logiciel, des secrets d'exploitation ou de l'infrastructure, sauf si un avenant d'hébergement dédié en dispose autrement pour

l'instance concernée.

Article 19 — Dispositions générales

- 19.1. **Loi applicable** : droit français. **Attribution de compétence** : tribunaux du ressort de **[À COMPLÉTER : siège de MOVELYTICS / clause du contrat commercial]**, sous réserve des règles d'ordre public et des droits des personnes concernées.
- 19.2. Toute modification du présent Accord se fait par écrit (y compris échange de PDF signés ou signature électronique).
- 19.3. La nullité d'une clause n'affecte pas les autres.
- 19.4. Le présent Accord peut être signé en deux exemplaires (ou électroniquement). Les annexes I à III en font partie intégrante.

Fait à _____, le _____

Pour le Client	Pour MOVELYTICS
Nom :	Nom :
Fonction :	Fonction :
Signature :	Signature :

Annexe I — Description du traitement

I.1 Finalités

Mise à disposition et exploitation de Noa dans Microsoft Teams pour les collaborateurs du Client : identification technique, rappels de pauses, cartes interactives, onglets Config et Bibliothèque, personnalisation fonctionnelle, statistiques **agrégées** de déploiement et d'usage, support, sécurité du Service, exercice des droits (export, effacement).

I.2 Nature des opérations

Collecte, enregistrement, conservation, consultation, adaptation (préférences), communication par voie de messages Teams et, le cas échéant, e-mail d'invitation calendrier, effacement, agrégation.

Pas d'appel à Microsoft Graph. Pas d'analyse des autres conversations, e-mails, fichiers, calendriers ou contacts M365. Pas d'agent LLM / Copilot.

I.3 Personnes concernées

Collaborateurs et autres utilisateurs du tenant Microsoft 365 du Client auxquels Noa est déployé ; référents internes du Client habilités au tableau de bord agrégé (`is_admin`).

I.4 Catégories de données

Catégorie	Exemples	Stockée ?
Identifiants Microsoft	<code>userId</code> Entra, <code>tenantId</code>	Oui
Identité professionnelle	nom, e-mail tels que transmis par Teams	Oui
Technique bot	référence de conversation (rappels proactifs)	Oui — exclue de l'export

Préférences	horaires, fuseau, zones corporelles, matériel, micro-learning, onboarding, invitations	Oui
Usage	pauses, sessions / favoris Bibliothèque, scores d'usage	Oui
Contrat / licence	statut de licence entreprise du tenant	Oui
Journal interne éditeur	accès support (identifiants techniques)	Oui (côté MOVELYTICS)
Humeur (mood)	—	Plus collectée ni enregistrée
Santé clinique / paiement carte	—	Non
Graph (mail, fichiers, annuaire étendu)	—	Non

I.5 Destinataires

Personnel habilité MOVELYTICS ; sous-traitants de l'annexe III ; le Client (agréats) ; l'utilisateur pour son propre compte (export / interface).

I.6 Durées

Voir article 10 : conservation pendant la relation (licence entreprise active/trial) ; effacement à la demande de la personne à tout moment ; **90 jours** après la fin de la dernière licence entreprise puis suppression du tenant.

I.7 Lieu

Backend et base : UE (Irlande, Heroku / PostgreSQL) **par défaut**, à la date du modèle. Un autre lieu ou une instance sur infrastructure du Client peut être convenu par avenant (article 17).

I.8 Identifiants techniques du Service (production)

- Manifeste Teams : `2a175964-2610-4c07-af50-d6a5d691c924`
- Bot / Entra : `8bf8b0c0-4eb2-44a0-92a2-aba236e64e52`
- Listing : WA200008766
- Hôte : `move-break-microsoft-teams-app-04b9b0a5156b.herokuapp.com`

Annexe II — Mesures techniques et organisationnelles

Mesures **effectives** à la date du modèle. Ce qui n'existe pas est indiqué comme tel (pas de remplissage fictif).

II.1 Pseudonymisation et minimisation

- Pas de Microsoft Graph ; permissions RSC vides.
- Tableau de bord Client limité aux agréats.
- Logs applicatifs bot sans e-mail ni nom ; messages non reconnus stockés en empreinte (hash) et longueur.
- Export utilisateur sans `conversation_reference`.
- Confirmation explicite pour l'effacement.

II.2 Chiffrement et transit

- HTTPS / TLS (terminaison hébergeur).
- HSTS (`max-age` 15 552 000 secondes, 180 jours).
- `X-Content-Type-Options: nosniff` ; `Referrer-Policy: no-referrer`.
- CSP `frame-ancestors` limitée aux origines Microsoft Teams / Office.

- Chiffrement au repos : celui du **PostgreSQL / disques Heroku** (mesure d'infrastructure prestataire, non un module applicatif MOVELYTICS distinct).

II.3 Confidentialité et intégrité

- JWT Azure Bot Service sur le canal messages.
- Requêtes SQL paramétrées.
- Limitation de débit sur les API hors canal bot.
- Secrets dans la configuration de l'hébergeur.
- Onglets identifiés par le contexte Teams (`userId`) — **SSO Entra d'onglet non activé** (vérification éditeur Microsoft en cours). Cette limite est connue et assumée.

II.4 Disponibilité et résilience

- Hébergement PaaS ; sauvegardes et PRA **du prestataire Heroku** pour PostgreSQL.
- MOVELYTICS ne documente pas, à ce jour, de RTO/RPO contractuels autonomes.
- Scheduler de rappels : indisponibilité possible en cas d'incident PaaS ou Microsoft Teams (dépendance plateforme).

II.5 Gouvernance

- Effectif restreint, besoin d'en connaître.
- Journal d'accès administration interne.
- Contact : `fabrice@move.lytics.fr`.
- **Aucun pentest ni aucune certification n'a été passé** à la date du modèle (ISO 27001, SOC 2, certification Microsoft 365 App Certification, ou équivalent). Les options sont explorées ; tout engagement de mise en conformité suppose que le Client ait transmis son référentiel (article 5.3).

II.6 Développement

- Pas de sous-traitance de développement du backend Teams.
- Tests automatisés internes (dont export/effacement et logique de rétention).
- Synchronisation Notion **désactivée** (non utilisée en production).

Annexe III — Sous-traitants ultérieurs autorisés

Entité	Rôle	Données concernées	Localisation principale	Transfert hors EEE
Microsoft Corporation / affiliées	Microsoft Teams, Azure Bot Service, Entra ID (identité du bot)	Messages de la conversation Noa, jetons, identifiants Teams	Selon DPA Microsoft (datacenters UE + administration mondiale possible)	Possible — DPA / CCT Microsoft
Salesforce / Heroku	PaaS, PostgreSQL managé	Ensemble des Données stockées du Service dans l'offre par défaut	Irlande (UE) à la date du modèle	Accès support possible — DPA Salesforce / Heroku
Brevo (Sendinblue)	E-mail transactionnel si Move Invitation activée	E-mail, contenu d'invitation calendrier	UE (prestataire français)	Selon DPA Brevo
Google (YouTube) / Vimeo	Lecteur vidéo si l'utilisateur lance une vidéo	Identifiants de lecture / métadonnées lecteur	Selon ces prestataires (souvent hors EEE)	Uniquement sur action utilisateur

Non utilisés dans l'application Teams à la date du modèle : Stripe (paiement), Notion (sync désactivée), Microsoft

Graph.

Heroku / Salesforce figure ici comme hébergeur **par défaut**. Il peut être remplacé, ou complété par une instance sur infrastructure du Client, uniquement par **avenant** (article 17). Dans ce cas l'annexe III est mise à jour (nouveau PaaS et/ou le Client comme hébergeur de l'instance dédiée).

Le Client peut demander copie ou lien des DPA publics de ces prestataires.

Fin du modèle de DPA.