

Note DORA — premier échange

Produit : Noa by MoveBreak (Microsoft Teams)

Éditeur : MOVELYTICS SASU

Version : 1.0 — 7 septembre 2026

Statut : position de discussion, **pas** un contrat DORA signé

Le règlement (UE) 2022/2554 (DORA) s’applique aux **entités financières** et, par ricochet, à leurs prestataires de services TIC. Il n’impose pas à une startup de trois personnes d’être d’emblée un « prestataire TIC critique » au sens du titre V. Cette note dit **ce que nous pouvons contractualiser aujourd’hui** et **ce que nous ne pouvons pas tenir**.

1. Nature du service au regard du SI bancaire

Noa est une application de **rappels de pauses bien-être** dans Microsoft Teams. Elle n’exécute pas d’opérations de paiement, de tenue de compte, de reporting prudentiel, d’authentification des clients de la banque, ni de messagerie métier interne.

Une interruption de Noa dégrade un service QVT. Elle ne devrait pas, en elle-même, empêcher l’entité de fournir ses **fonctions essentielles**.

Conséquence proposée : Noa est un prestataire TIC **non critique** et, selon l’analyse du client, éventuellement **non important**. **Seul le client** procède à cette qualification dans son registre des prestataires. Nous ne la contestons pas par principe ; nous ne l’anticipons pas non plus.

Si le Client (groupe ou entité) nous classait néanmoins prestataire **important** ou **critique**, les obligations (tests de résilience, audit, sous-traitance en cascade, etc.) dépassent ce que MOVELYTICS peut garantir **aujourd’hui**. Il faudrait alors un avenant, un calendrier et probablement un autre niveau de maturité (pentest, processus) — pas une signature immédiate du régime complet.

2. Clauses que nous pouvons accepter dès maintenant

Sous réserve du contrat commercial et du DPA :

Thème DORA (esprit)	Position MOVELYTICS
Description du service	Annexe technique + fiche sécurité
Localisation / sous-traitance	Liste des sous-traitants ultérieurs (Heroku, Microsoft, Brevo si utilisé, lecteurs vidéo) ; notification des ajouts significatifs
Accès et sécurité	Mesures du DPA ; pas de Graph ; PaaS UE
Notification d’incident de sécurité / violation de données	Information du client sans délai injustifié (voir DPA)
Coopération raisonnable	Réponses écrites, visio, questionnaires — dans une limite compatible avec un effectif de 3
Réversibilité / sortie	Export JSON individuel déjà en self-service ; restitution agrégée ou suppression du tenant selon instructions ; purge 90 jours après fin de licence
Droit d’audit	Audit documentaire raisonnable, préavis, pendant les heures ouvrées, pas plus d’une fois par an hors incident, coûts du client sauf faute grave de l’éditeur
Loi applicable	Droit français, RGPD ; pas d’invention de droit américain sur les données UE

3. Clauses que nous ne pouvons pas accepter en l’état

Les formuler clairement évite un blocage plus tard.

Demande fréquente	Pourquoi ce n'est pas tenable aujourd'hui
Pentest à la demande sous 30 jours, correction critical/high sous 30 jours, rapport livré au groupe	Aucun pentest n'existe ; pas d'équipe sécu dédiée
SOC 24/7, astreinte, RTO/RPO contractuels chiffrés maison	Dépendance PaaS ; pas de centre d'opérations
ISO 27001 / SOC 2 en vigueur	Absents
Droit d'audit illimité , sur site, y compris chez Heroku / Microsoft, à nos frais	Nous n'avons pas le pouvoir d'imposer un audit à Salesforce ou Microsoft ; coût disproportionné
Interdiction de Microsoft Teams	Le produit est une app Teams ; le canal Bot Service n'est pas substituable
Interdiction d' Heroku / PaaS Salesforce	Négociable : autre PaaS accepté par le client, ou instance dédiée sur infra client, par avenant (pas l'offre par défaut)
Tests d'intrusion du client sur production sans encadrement	À discuter (fenêtre, périmètre, pas de déni de service) ; pas un chèque en blanc
Qualification volontaire « TIC critique » et régime titre V DORA	Inadapté au service et à la taille
Transfert immédiat de tout le code et des secrets « pour réversibilité »	Réversibilité = données + arrêt du service, pas cession du logiciel

4. Sous-traitance en cascade

Chaîne actuelle, volontairement courte :

1. MOVELYTICS (éditeur)
2. Microsoft (canal Teams / Bot)
3. Heroku / Salesforce (hébergement et Postgres) — **par défaut**, substituable (autre PaaS ou instance sur infra client)
4. Brevo (e-mail, optionnel)
5. YouTube / Vimeo (lecture vidéo, optionnel, déclenchée par l'utilisateur)

Nous n'ajoutons pas de sous-traitant de développement. Un changement **significatif** (nouvel hébergeur, instance dédiée chez le client, nouvel outil d'e-mail, rétablissement d'un prestataire de paiement dans Teams) serait notifié / cadré selon le DPA (article 17 du modèle).

Nous ne pouvons pas garantir que Microsoft ou Salesforce n'ont **aucun** sous-traitant propre : leurs DPA publics s'appliquent.

5. Stratégie de sortie (réversibilité)

À la fin du contrat :

1. Le client peut demander une **restitution** des données personnelles du tenant dans un format usuel (export JSON / CSV raisonnable), dans un délai convenu.
2. À défaut d'instruction, conservation **90 jours** puis **suppression** des comptes du tenant (hors obligation légale et hors environnements de démo internes de l'éditeur).
3. Les collaborateurs **ne recréent pas** leur compte eux-mêmes après cette purge ; un redéploiement relèverait d'un nouveau contrat et de la DSI.
4. Les statistiques réellement anonymisées peuvent être conservées par MOVELYTICS pour amélioration du service.

Il n'existe pas, dans l'offre SaaS actuelle, de « VM à rapatrier » : le service n'est pas hébergé chez le client. **Si** le client exige une instance sur son infrastructure, cela se discute par avenant d'hébergement (autre PaaS homologué, ou serveurs + base lui appartenant), ce n'est pas le déploiement standard.

6. Proposition pour la suite des échanges

1. Qualifier Noa dans le registre des prestataires du client (**proposition : non critique**).
2. **Dès ce premier échange** : nous transmettre **l'intégralité** des exigences applicables à une solution tierce (pentest, ISO / SOC 2, certification Microsoft, questionnaires, clauses d'audit, qualification TIC importante / critique, délais de correction, **PaaS imposé ou instance sur votre infrastructure**, etc.). À ce jour **aucun pentest ni aucune certification n'a été passé** ; nous explorons les options. L'hébergement actuel est Heroku (UE) ; nous sommes ouverts à un autre PaaS que vous acceptez, ou à une instance dédiée sur vos serveurs / votre base, **dans un cadre écrit**. Avec le référentiel, nous indiquons ce qui est finançable et dans quel délai, ou ce qui ne le sera pas.
3. Signer le **DPA article 28** + contrat commercial.
4. Garder DORA dans un **avenant court** (coopération, incidents, sortie, sous-traitants) plutôt que d'annexer un contrat prestataire critique type GIE, **sauf** si le point 2 montre que le client exige ce régime — auquel cas il faut le savoir **avant**, pas après un pilote.