



Incident eSignFlow : aide au remplissage de votre notification au CCB

Vanden Broele · version du 27 octobre 2026 · confidentiel, réservé aux clients d'eSignFlow

Ce document suit, champ par champ, le formulaire de notification en ligne du Centre pour la Cybersécurité Belgique (CCB) sur notif.safeonweb.be. Pour les faits relevant de Vanden Broele, vous pouvez reprendre le texte tel quel. Le texte entre **[]** est à compléter par vos soins, le plus souvent avec les chiffres de notre courrier du 25 octobre 2026 ou de l'export pour votre organisation.

Les champs de texte libre du CCB sont limités à 500 caractères. Les textes ci-dessous restent dans cette limite si vous complétez brièvement les champs entre **[]**.

Délai : obligatoire uniquement pour les entités essentielles et importantes au sens de NIS2 (24 heures, 72 heures, rapport final dans un délai d'un mois). Les autres organisations peuvent notifier volontairement via notif.safeonweb.be.

Champs du formulaire de notification

Le formulaire du CCB est en anglais ; les intitulés des champs sont repris tels qu'ils figurent sur notif.safeonweb.be. Vous pouvez répondre en français. Lors de la notification à 72 heures, vous donnez une première évaluation ; dans le rapport final, une évaluation détaillée.

Champ du formulaire	À compléter
DÉCLARANT	
Concerning / How is the organisation defined / Main sector	[Vos propres données. Si vous ne relevez pas de NIS2, choisissez 'Voluntary Notification' comme type de notification.]
What type of NIS2 incident notification are you submitting?	[24h initial report, 72h/intermediate report ou Final Report]
INCIDENT	
Tracking Reference	[Votre propre référence CCB, à partir de la deuxième notification]
Do you believe this incident is the result of malicious intent?	Yes
Incident Type	Data leak. Également Account compromise si notre courrier indique que la clé API de votre organisation a été utilisée de manière abusive.
When did the incident take place?	22/10/2026
Describe the incident	Chez notre fournisseur Vanden Broele (eSignFlow, signature électronique), un environnement d'administration était accessible depuis l'extérieur. Le 22/10/2026, un attaquant externe y a lu des clés API et a consulté via l'API des données de notre organisation, du 22/10 03:48 au 23/10 11:17 : [données de documents / signataires / liste des utilisateurs / documents téléchargés] . Vanden Broele a constaté l'incident le 23/10 à 09:30 et nous a informés le jour même.
Please provide an assessment of the severity of the incident	Atteinte vraisemblablement malveillante à la confidentialité de données à caractère personnel chez un prestataire. Concernés : noms, adresses e-mail, données de documents avec codes d'accès et, pour les signataires, le numéro de Registre national. Nos propres réseaux et systèmes n'ont pas été touchés. eSignFlow était indisponible du 23/10 12:15 au 24/10 vers 20:00.
What are the consequences of the incident?	[Nombre] documents dont les données ont été consultées, [nombre] signataires, [nombre] utilisateurs et [nombre] documents téléchargés. Risque de phishing ciblé chez les membres du personnel, signataires et destinataires. eSignFlow était temporairement indisponible (23/10 12:15 au 24/10 vers 20:00) ; les intégrations ne fonctionnent qu'avec une nouvelle clé.
What caused the incident?	Chez le fournisseur : un environnement d'administration était protégé par un contrôle n'autorisant que le réseau interne. Après une modification, tout le trafic passait par un reverse proxy, si bien que les requêtes externes semblaient internes. Cet environnement contenait

	des clés API. L'analyse des causes par un partenaire spécialisé externe (forensique) est attendue semaine du 2/11/2026.
Do you believe this incident might lead to cross-border issues?	No
Have you reported the incident to the police?	[Votre propre plainte.] Vanden Broele a déposé plainte le 26/10/2026.
Do you need support, analysis or advice from the CCB?	[Votre choix, en général No]
What actions did you take?	Fournisseur : service hors ligne, environnement d'administration fermé, adresses IP de l'attaquant bloquées, remplacement de toutes les clés API, des secrets de webhook et de la connexion itsme, nouveau mot de passe pour chaque document consulté, journaux sécurisés, enquête forensique externe. Nous : [nouvelles clés pour les intégrations, utilisateurs mis en garde contre le phishing, personnes concernées informées] .
Is the incident now resolved?	Yes : maîtrisé le 23/10/2026 à 12:15, toutes les clés remplacées le 24/10/2026. L'enquête se poursuit.
Was MFA applied to your impacted environment?	[Votre choix.] Pour information : l'attaquant a utilisé des clés API, sans connexion via des comptes utilisateurs.
FURTHER INFORMATION (rapport final)	
When was the incident detected? / How was the incident detected?	[Date et heure de notre première notification, 23/10/2026.] Notification par le fournisseur Vanden Broele.
Provide a detailed timeline with all actions taken	22/10 03:48 première reconnaissance ; 22/10 07:00 lecture de l'environnement d'administration ; 22/10 08:41 première consultation avec une clé ; 23/10 09:30 constat chez le fournisseur ; 23/10 11:17 dernière activité ; 23/10 12:15 eSignFlow hors ligne ; 23/10 première notification à notre organisation ; 24/10 toutes les clés remplacées, eSignFlow de nouveau en ligne vers 20:00 ; 25/10 courrier avec nos données. [Ajoutez vos propres actions.]
Which communication occurred in response to the incident?	Du fournisseur vers nous : courriel du 23/10/2026 (première notification), courrier du 25/10/2026 (constatations par organisation), courriel du 26/10/2026 (communiqué et lettres types). [Votre propre communication.]
What preventive measures were in place at the time of the incident?	Chez le fournisseur : système de management certifié ISO 27001 ; environnement d'administration ouvert uniquement au réseau interne ; accès API uniquement avec une clé par organisation. [Vos propres mesures.]
What corrective measures were taken as a result of the incident?	eSignFlow hors ligne le 23/10/2026 à 12:15 ; environnement d'administration fermé depuis l'extérieur ; adresses IP de l'attaquant bloquées ; remplacement de toutes les clés API, des secrets de webhook, de la connexion itsme et des clés système internes ; nouveau mot de passe pour chaque document consulté ; suppression des clés et droits créés par l'attaquant ; journaux sécurisés.
What new (adapted) preventive measures were implemented after the incident?	Chez le fournisseur : analyse des causes par vecteur d'attaque par un partenaire forensique externe ; correction définitive de la protection ; contrôle de tous les environnements d'administration. [Vos propres mesures.]
What lessons were learned from the incident?	[Vos propres enseignements.]
CONTACT	
Where did the incident take place?	Chez le fournisseur : eSignFlow (SaaS de Vanden Broele SA), Belgique.