



Incident eSignFlow : aide au remplissage de votre notification à l'APD

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

Pour les données traitées dans eSignFlow, vous êtes responsable du traitement et Vanden Broele est sous-traitant. C'est donc à vous de décider si vous notifiez l'incident. Ce document suit, champ par champ, le formulaire de notification en ligne de l'Autorité de protection des données (APD). 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 de l'APD sont limités à 100 caractères, sauf mention contraire. Les textes ci-dessous restent dans cette limite si vous complétez brièvement les champs entre **[]**.

Délai : notifier dans les 72 heures après avoir pris connaissance de la violation. La partie 1 peut être introduite sans compte ; la partie 2 suit dans les 21 jours via le compte entreprise. Si vous relevez de l'Organe de contrôle de l'information policière (COC), c'est auprès de lui que vous notifiez.

Champs du formulaire de notification

Ordre et intitulés du formulaire de notification. Les champs relatifs à votre propre organisation (nom, adresse, personne de contact, DPO) ne sont pas repris ici.

Champ du formulaire	À compléter
INTRODUCTION	
Avez-vous également notifié la violation de données auprès d'autres contrôleurs nationaux ... ? Ou avez-vous déposé plainte à la police et/ou au parquet ?	[Vos propres notifications.] Les notifications de Vanden Broele ne sont pas à mentionner ici.
ORGANISATION	
La violation de données a-t-elle eu lieu dans le cadre d'un traitement qui a été confié à un sous-traitant ?	Oui
De quel sous-traitant s'agit-il ?	Vanden Broele SA, Lieven Bauwensstraat 35, 8200 Brugge, numéro d'entreprise 0451.355.351
NIVEAU INTERNATIONAL	
La violation a-t-elle des conséquences pour des personnes concernées dans plusieurs pays ?	Non [sauf si votre export mentionne des signataires de nationalité ou de résidence étrangère]
LIGNE DU TEMPS	
Quand la fuite de données s'est-elle produite ?	La date et l'heure exactes auxquelles la violation de données a eu lieu sont connues
Date et heure auxquelles la violation de données s'est produite	22/10/2026 07:00
Date et heure de la découverte de la violation de données	[Date et heure de réception de notre première notification : 23/10/2026, heure selon le courriel de Vanden Broele.]
Manière dont la violation de données a été découverte	Notification externe > Par un fournisseur ou un sous-traitant > Vanden Broele SA, [date et heure de la première notification]
Justification de la notification tardive (uniquement si d'application)	[Votre propre justification.] Pour information : notre courrier reprenant les constatations par organisation date du 25/10/2026.
Quand la violation de données a-t-elle été résolue ?	La violation de données a été résolue : 23/10/2026 12:15 (eSignFlow mis hors ligne)
TRAITEMENT	
Finalités pour lesquelles les données à caractère personnel sont traitées	Signature électronique et transmission de documents de l'organisation via eSignFlow.
Nature des données à caractère personnel qui ont été touchées par la violation de données	À cocher selon notre courrier du 25/10/2026 : - Données d'identification (noms des utilisateurs, signataires et destinataires) - Données d'identification électroniques (adresses e-mail)

	- Profession et emploi (fonctions dans les données des documents), le cas échéant - Numéro d'identification unique > Numéro national (numéro de Registre national), si notre courrier mentionne des signataires - Code d'accès (code d'accès et mot de passe des documents) - Autres : contenu de documents téléchargés, uniquement si notre courrier mentionne des documents téléchargés
Catégories particulières (article 9.1 du RGPD) et données relatives aux condamnations pénales et aux infractions (article 10 du RGPD)	[Votre appréciation, sur la base des titres de documents dans l'export, p. ex. dossiers SAC, dossiers du personnel ou documents relatifs à des mineurs.]
Le nombre exact de personnes concernées est-il connu ? / Nombre minimal et maximal	Non. Minimum : [nombre de signataires + nombre d'utilisateurs selon notre courrier]. Maximum : [minimum + personnes figurant dans les données des documents, selon l'export].
Groupes de personnes concernées touchées par la violation de données	Travailleurs/collaborateurs (membres du personnel et mandataires), Citoyens, Autres : signataires et destinataires externes [à adapter selon votre export]
Le degré et la possibilité d'identification des personnes concernées	Données directement identifiables (nom avec adresse e-mail ou numéro de Registre national)
CAUSES	
La cause de la violation de données était	Externe (chez le sous-traitant)
La violation de données a été causée par	Un acte technique lié au système
L'intention derrière la violation de données était	Action malveillante
Quelle est la nature de la violation de données ?	Violation de confidentialité. Également violation de disponibilité : eSignFlow était hors ligne du 23/10/2026 12:15 au 24/10/2026 vers 20:00.
Type de violation de données	Cartes, applications ou localisation de réseau contenant des données à caractère personnel accessibles en dehors de l'organisation
Peut-on vérifier, sur la base des fichiers de journalisation, combien de personnes ont eu accès ... ?	Oui, sur la base des journaux disponibles : ils montrent les adresses IP d'un seul attaquant.
Peut-on vérifier, sur la base de fichiers de journalisation, à quel moment des personnes ont eu accès ... ?	Oui : du 22/10/2026 03:48 au 23/10/2026 11:17.
Peut-on vérifier si l'on a effectué des téléchargements ou des copies similaires ... ?	Oui pour les téléchargements (voir notre courrier). Copie du contenu consulté : non vérifiable.
Avez-vous (ou un acteur externe) enquêté sur la cause et/ou l'ampleur de la violation de données ? / Date probable des résultats	Oui : partenaire forensique externe depuis le 26/10/2026. Analyse attendue semaine du 2/11/2026.
Résumé de la violation de données (max. 2 500 caractères)	eSignFlow est un service de signature électronique de Vanden Broele SA, qui agit à ce titre comme sous-traitant de [nom de l'organisation]. Un environnement d'administration d'eSignFlow, destiné au suivi des tâches en arrière-plan, était accessible depuis l'extérieur. Le 22/10/2026, un attaquant externe inconnu y a lu des clés API. Avec ces clés, il s'est fait passer pour un utilisateur via l'API et a consulté des données, du 22/10/2026 03:48 au 23/10/2026 11:17. Vanden Broele a constaté l'incident le 23/10/2026 à 09:30, a mis eSignFlow hors ligne le même après-midi et nous en a informés le jour même. Le 25/10/2026, nous avons reçu un courrier reprenant les constatations pour notre organisation. Pour notre organisation, il s'agit de : [à reprendre du courrier du 25/10/2026 : nombre de documents dont les données ont été consultées, nombre de signataires, liste des utilisateurs oui/non, nombre de documents téléchargés]. Pour les signataires, l'attaquant a pu consulter le nom, le pays et le numéro de Registre national. Celui-ci figurait sous une forme convertie, facile à reconvertir. Pour les destinataires et les autres personnes figurant dans les données des documents, il s'agissait du nom, de l'adresse e-mail et du titre du document, avec le code d'accès, ce qui rendait le contenu accessible. Il n'est pas possible d'établir pour chaque document si l'attaquant en a effectivement ouvert le contenu. Vanden Broele a renouvelé toutes les clés, attribué un nouveau mot

	de passe à chaque document consulté et fermé l'accès à l'environnement d'administration. Un partenaire forensique externe enquête sur l'incident. L'analyse des causes est attendue dans la semaine du 2/11/2026.
GESTION (mesures)	
Quelles mesures spécifiques étaient en vigueur afin de protéger les données à caractère personnel affectées ?	Chez le sous-traitant : système de management certifié ISO 27001 ; environnement d'administration ouvert uniquement au réseau interne ; accès API uniquement avec une clé par organisation. Chez nous : contrat de sous-traitance avec Vanden Broele [et vos propres mesures] .
Quelles mesures nouvelles/complémentaires ont été prises spécifiquement suite à la violation de données ?	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.
Quelles mesures nouvelles/complémentaires seront spécifiquement prises à l'avenir ?	Chez le sous-traitant : analyse des causes par vecteur d'attaque par un partenaire forensique externe ; correction définitive de la protection ; contrôle de tous les environnements d'administration. Chez nous : [suivi du sous-traitant, mise en garde des utilisateurs contre le phishing, nouvelles clés pour les intégrations] .
RISQUE	
Méthode d'évaluation des risques / Résultat de l'analyse / Impact/conséquences pour les personnes concernées	[Votre propre appréciation.] À titre indicatif : le risque est le plus élevé pour les personnes figurant dans un document téléchargé et pour les signataires (numéro de Registre national). La principale conséquence est le phishing et l'usurpation d'identité.
COMMUNICATION	
Avez-vous déjà notifié la violation aux personnes concernées ?	[Votre décision.] Vanden Broele ne contacte pas directement les personnes concernées. Une lettre type comprenant un module par groupe est disponible via ciso@vandenbroele.be .
ANNEXES	
Annexes à charger	Copie datée de la notification externe : le courrier de Vanden Broele du 25/10/2026. Copie datée du rapport d'enquête : suivra après l'analyse. Copie datée de la communication aux personnes concernées : votre courrier ou avertissement général.

Questions

Vous pouvez demander l'export pour votre organisation et la lettre type destinée aux personnes concernées via ciso@vandenbroele.be.