Incident eSignFlow: invulhulp voor uw melding bij het CCB

Vanden Broele · versie 27 oktober 2026 · vertrouwelijk, enkel voor klanten van eSignFlow

Deze invulhulp volgt het online meldformulier van het Centrum voor Cybersecurity België (CCB) op notif.safeonweb.be, veld per veld. Waar het om feiten van Vanden Broele gaat, kunt u de tekst overnemen. Tekst tussen **[ ]** vult u zelf in, meestal met de cijfers uit onze brief van 25 oktober 2026 of uit de export voor uw organisatie.

De vrije tekstvelden van het CCB zijn beperkt tot 500 tekens. De teksten hieronder blijven binnen die grens zolang u de velden tussen **[ ]** kort houdt.

Termijn: verplicht enkel voor essentiële en belangrijke entiteiten onder NIS2 (24 uur, 72 uur, eindverslag binnen een maand). Andere organisaties kunnen vrijwillig melden via notif.safeonweb.be.

Velden van het meldformulier

Het CCB-formulier is in het Engels; de veldnamen staan zoals op notif.safeonweb.be. U mag in het Nederlands antwoorden. Bij de 72-uursmelding geeft u een eerste beoordeling, in het eindverslag een gedetailleerde.

Veld in het formulier	Wat u invult
MELDER	
Concerning / How is the organisation defined / Main sector	**[Uw eigen gegevens. Valt u niet onder NIS2, dan kiest u bij het meldtype 'Voluntary Notification'.]**
What type of NIS2 incident notification are you submitting?	**[24h initial report, 72h/intermediate report of Final Report]**
INCIDENT	
Tracking Reference	**[Uw eigen CCB-referentie, vanaf de tweede melding]**
Do you believe this incident is the result of malicious intent?	Yes
Incident Type	Data leak. Ook Account compromise als onze brief vermeldt dat de API-sleutel van uw organisatie misbruikt werd.
When did the incident take place?	22/10/2026
Describe the incident	Bij onze leverancier Vanden Broele (eSignFlow, e-signing) was een beheeromgeving van buitenaf bereikbaar. Een externe aanvaller las er op 22/10/2026 API-sleutels uit en vroeg daarmee via de API gegevens van onze organisatie op, van 22/10 03:48 tot 23/10 11:17: **[documentgegevens / ondertekenaars / gebruikerslijst / gedownloade documenten]**. Vanden Broele stelde het incident op 23/10 09:30 vast en bracht ons dezelfde dag op de hoogte.
Please provide an assessment of the severity of the incident	Vermoedelijk kwaadwillige aantasting van de vertrouwelijkheid van persoonsgegevens bij een dienstverlener. Betrokken: namen, e-mailadressen, documentgegevens met toegangscodes en, bij ondertekenaars, het rijksregisternummer. Onze eigen netwerken en systemen zijn niet geraakt. eSignFlow was van 23/10 12:15 tot 24/10 omstreeks 20:00 onbeschikbaar.
What are the consequences of the incident?	**[Aantal]** documenten waarvan gegevens werden opgevraagd, **[aantal]** ondertekenaars, **[aantal]** gebruikers en **[aantal]** gedownloade documenten. Risico op gerichte phishing bij medewerkers, ondertekenaars en ontvangers. eSignFlow was tijdelijk onbeschikbaar (23/10 12:15 tot 24/10 omstreeks 20:00); koppelingen werken pas weer met een nieuwe sleutel.
What caused the incident?	Bij de leverancier: een beheeromgeving was beveiligd met een controle die enkel het eigen netwerk toeliet. Na een wijziging liep alle verkeer via een reverse proxy, waardoor ook verzoeken van buitenaf intern leken. In die omgeving stonden API-sleutels. De oorzaakanalyse per aanvalsweg door een externe forensische partner wordt verwacht in de week van 2/11/2026.
Do you believe this incident might lead to cross-border issues?	No

Have you reported the incident to the police?	**[Uw eigen aangifte.]** Vanden Broele deed aangifte op 26/10/2026.
Do you need support, analysis or advice from the CCB?	**[Uw keuze, doorgaans No]**
What actions did you take?	Leverancier: dienst offline, beheeromgeving afgesloten, IP-adressen van de aanvaller geblokkeerd, alle API-sleutels, webhookgeheimen en de itsme-koppeling vervangen, nieuw wachtwoord voor elk opgevraagd document, logs veiliggesteld, extern forensisch onderzoek. Wij: **[nieuwe sleutels voor koppelingen, gebruikers gewaarschuwd voor phishing, betrokkenen ingelicht]**.
Is the incident now resolved?	Yes: ingeperkt op 23/10/2026 12:15, alle sleutels vervangen op 24/10/2026. Het onderzoek loopt.
Was MFA applied to your impacted environment?	**[Uw keuze.]** Ter info: de aanvaller gebruikte API-sleutels, geen aanmelding met gebruikersaccounts.
FURTHER INFORMATION (eindverslag)	
When was the incident detected? / How was the incident detected?	**[Datum en uur van onze eerste melding, 23/10/2026.]** Melding door de leverancier Vanden Broele.
Provide a detailed timeline with all actions taken	22/10 03:48 eerste verkenning; 22/10 07:00 uitlezen van de beheeromgeving; 22/10 08:41 eerste opvraging met een sleutel; 23/10 09:30 vaststelling bij de leverancier; 23/10 11:17 laatste activiteit; 23/10 12:15 eSignFlow offline; 23/10 eerste melding aan ons; 24/10 alle sleutels vervangen, eSignFlow rond 20:00 weer online; 25/10 brief met onze gegevens. **[Uw eigen acties toevoegen.]**
Which communication occurred in response to the incident?	Leverancier aan ons: mail 23/10/2026 (eerste melding), brief 25/10/2026 (vaststellingen per organisatie), mail 26/10/2026 (statement en modelbrieven). **[Uw eigen communicatie.]**
What preventive measures were in place at the time of the incident?	Bij de leverancier: ISO 27001-gecertificeerd beheersysteem; beheeromgeving enkel open voor het interne netwerk; API-toegang enkel met een sleutel per organisatie. **[Uw eigen maatregelen.]**
What corrective measures were taken as a result of the incident?	eSignFlow offline op 23/10/2026 12:15; beheeromgeving van buitenaf afgesloten; IP-adressen van de aanvaller geblokkeerd; alle API-sleutels, webhookgeheimen, de itsme-koppeling en interne systeemsleutels vervangen; nieuw wachtwoord voor elk opgevraagd document; door de aanvaller aangemaakte sleutels en rechten verwijderd; logs veiliggesteld.
What new (adapted) preventive measures were implemented after the incident?	Bij de leverancier: oorzaakanalyse per aanvalsweg door een externe forensische partner; definitieve correctie van de afscherming; controle van alle beheeromgevingen. **[Uw eigen maatregelen.]**
What lessons were learned from the incident?	**[Uw eigen lessen.]**
CONTACT	
Where did the incident take place?	Bij de leverancier: eSignFlow (SaaS van Vanden Broele NV), België.