

Notification d'incident au CCB

Trois échéances, trois contenus différents. Ce document sert de trame à remplir pendant l'incident : il n'est utile que s'il est pré-rempli *avant*.

À pré-remplir maintenant, pas pendant la crise

Numéro d'entreprise (BCE)	
Point de contact incident 24/7	
Téléphone et adresse de secours	
Identifiant du portail CCB	
Qui décide de notifier	
Suppléant	

Échéance 1 — alerte précoce, sous 24 heures

Point de départ : le moment où vous avez **connaissance** de l'incident significatif, pas celui où il a commencé. À ce stade, on n'attend ni analyse ni cause racine.

CHAMP	CONTENU
Date et heure de détection	
Entité concernée (BCE)	
Nature suspectée	
Origine : malveillante ou non	
Impact transfrontalier possible	

Échéance 2 — notification, sous 72 heures

Elle complète l'alerte et engage une première appréciation.

CHAMP	CONTENU
Mise à jour de l'appréciation initiale	
Gravité et impact constatés	
Indicateurs de compromission	
Services touchés et nombre d'utilisateurs	

CHAMP	CONTENU
Mesures d'atténuation en cours	

Échéance 3 — rapport final, sous 1 mois

CHAMP	CONTENU
Description détaillée de l'incident	
Type de menace et cause racine	
Mesures appliquées et en cours	
Impact transfrontalier le cas échéant	
Enseignements et plan d'action	

Ne pas confondre avec le RGPD

Si l'incident touche des données à caractère personnel, une notification distincte à l'**Autorité de protection des données** est due dans les **72 heures**, avec un contenu et un destinataire différents. Les deux régimes se cumulent : l'un ne dispense pas de l'autre.

Après l'incident

- Journaliser les actions au fil de l'eau, horodatées — c'est ce qui permettra de reconstituer, et ce que l'inspecteur demandera.
- Préserver les preuves avant de redémarrer : un redémarrage efface la mémoire vive.
- Tenir le registre des incidents : son absence est un constat en soi.