

Pack de modèles de notification de violation RGPD

Notification à l'autorité (article 33) · Lettre aux personnes concernées (article 34) · Registre des violations (article 33(5))

MODÈLE GRATUIT — DOCX · PDF · MD | Version 1.0 · Mise à jour 2026-07-22

Document A — à déposer auprès de votre autorité de contrôle sous 72 heures après la prise de connaissance (RGPD, art 33).

Document B — à envoyer aux personnes concernées dans les meilleurs délais lorsque le risque est élevé (RGPD, art 34).

Document C — consignez chaque violation, notifiée ou non (RGPD, art 33(5)).

Document D — l'aide à la décision notifier-ou-non.

France : notification à la CNIL via le téléservice en ligne. Royaume-Uni : à l'ICO (formulaire en ligne / téléphone). Norvège : au Datatilsynet via Altinn.

Transfrontière dans l'UE/EEE : notifiez votre autorité de contrôle chef de file (art 56).

Document A — Notification à l'autorité de contrôle (article 33)

Complétez chaque section. Les sections 2 à 5 correspondent à l'article 33(3)(a)–(d) — le contenu minimal légal. L'horloge des 72 heures court à partir de la prise de connaissance (lignes directrices 9/2022 du CEPD) : le moment où une personne responsable conclut avec une certitude raisonnable que des données personnelles ont été compromises.

A.1 Détails du dépôt

À (autorité de contrôle)	Autorité compétente ; autorité de contrôle chef de file si transfrontière (art 56)
De (responsable du traitement)	Dénomination de l'entité juridique et adresse du siège
Référence de l'incident	ID interne, p. ex. BREACH-2026-007
Type de notification	Initiale / Mise à jour / Finale (notification échelonnée, art 33(4))
Déposée le (date & heure)	Horodatage de ce dépôt

A.2 Prise de connaissance et chronologie (art 33(1))

Horodatage de prise de connaissance	Quand une personne responsable a conclu qu'une violation s'était probablement produite — démarre l'horloge des 72 heures
Comment nous en avons eu connaissance	Alerte, avis d'un sous-traitant au titre de l'art 33(2), signalement d'un client, constat d'audit...
Motifs du retard	OBLIGATOIRE si ce dépôt intervient plus de 72 heures après la prise de connaissance ; sinon n/a

A.3 Nature de la violation (art 33(3)(a))

Ce qui s'est passé	Décrivez l'incident et sa cause ; violation de confidentialité, d'intégrité et/ou de disponibilité
Catégories de personnes concernées	P. ex. clients, salariés, utilisateurs finaux des clients
Nombre approx. de personnes concernées	Nombre ou fourchette ; à mettre à jour dans les dépôts ultérieurs si cela change
Catégories de données personnelles	P. ex. données de contact, identifiants, données financières — signaler explicitement les catégories particulières (art 9)
Nombre approx. d'enregistrements	Nombre ou fourchette

A.4 Point de contact (art 33(3)(b))

DPO / point de contact	Nom, rôle, e-mail, téléphone — où l'autorité peut obtenir davantage d'informations
------------------------	--

A.5 Conséquences probables (art 33(3)(c))

Conséquences probables	Préjudices réalistes : usurpation d'identité, fraude, perte financière, atteinte à la réputation, exposition de catégories particulières
-------------------------------	--

A.6 Mesures prises ou proposées (art 33(3)(d))

Confinement & remédiation	Ce qui a été fait pour remédier à la violation
Atténuation des effets négatifs	Mesures réduisant le préjudice pour les personnes concernées, p. ex. réinitialisation forcée des mots de passe, révocation des identifiants

A.7 Position sur la communication aux personnes concernées

Évaluation du risque	Risque peu probable / risque / risque élevé — avec un bref raisonnement
Position au titre de l'article 34	Communication envoyée ou prévue (date), ou exception : 34(3)(a) données incompréhensibles, 34(3)(b) risque écarté, 34(3)(c) communication publique

A.8 Traitement transfrontière (art 56)

Transfrontière ?	Des personnes concernées dans plus d'un État membre sont-elles affectées ?
Fondement de l'autorité chef de file	Raisonnement d'établissement principal identifiant l'autorité de contrôle chef de file

Document B — Communication aux personnes concernées (article 34)

Requise dans les meilleurs délais lorsque la violation est susceptible d'engendrer un risque ÉLEVÉ. En termes clairs et simples ; doit contenir au moins le point de contact, les conséquences probables et les mesures (art 34(2) → art 33(3)(b),(c),(d)). Remplacez le texte entre crochets ; faites des phrases courtes ; évitez le jargon.

Objet	Information importante concernant la sécurité de vos données personnelles
Ce qui s'est passé	[Une ou deux phrases en langage simple : ce qui s'est passé, quand cela a été découvert et contenu.]
Quelles informations sont concernées	[Les catégories des données du destinataire affectées. Indiquez clairement ce qui n'a PAS été affecté, p. ex. les données de paiement.]
Ce que cela peut signifier pour vous	[Les conséquences réalistes — p. ex. des e-mails d'hameçonnage qui semblent provenir de nous, des tentatives de connexion.]
Ce que nous faisons	[Confinement, enquête, notification de l'autorité de contrôle, améliorations de sécurité.]
Ce que vous pouvez faire	[Mesures concrètes : réinitialisez votre mot de passe, activez l'authentification à deux facteurs, méfiez-vous des e-mails suspects, surveillez vos relevés.]
Où obtenir plus d'informations	[DPO / point de contact : nom, e-mail, téléphone — et une page d'état si disponible.]
Conclusion	Nous vous présentons nos excuses pour l'inquiétude que cet incident peut causer. Nous vous tiendrons informé(e) de l'avancement de notre enquête.

Variante communication publique (art 34(3)(c))

Si contacter individuellement chaque personne concernée exigerait des efforts disproportionnés, publiez le même contenu sous forme de communication publique (bandeau sur le site web, communiqué de presse) informant les personnes concernées de manière tout aussi efficace — et consignez le choix du canal et le raisonnement dans le document C.

Document C — Fiche de registre interne des violations (article 33(5))

Complétez une fiche par incident — y compris pour les violations que vous décidez de NE PAS notifier. Ce registre est le moyen par lequel une autorité de contrôle vérifie la conformité à l'article 33.

Référence de l'incident	ID interne
Horodatage / mode de prise de connaissance	Quand l'horloge a démarré et ce qui a déclenché la prise de connaissance
Faits de la violation	Nature, cause, personnes concernées et enregistrements affectés
Effets	Conséquences réelles et probables observées

Évaluation du risque & raisonnement	Risque peu probable / risque / risque élevé — et pourquoi
Autorité notifiée ?	Oui (date, référence) / Non — raisonnement : peu susceptible d'engendrer un risque
Personnes concernées informées ?	Oui (date, canal) / Non — quelle exception de l'art 34(3) et pourquoi
Avis du sous-traitant (art 33(2))	Quel sous-traitant nous a informés et quand — si la violation a pris naissance chez un sous-traitant
Mesures correctives	Ce qui a été corrigé, changé ou amélioré en conséquence
Journal des dépôts	Notifications initiale / mise à jour / finale : dates et références

Document D — Aide à la décision notifier-ou-non

Situation	Ce que vous devez produire
Violation peu susceptible d'engendrer un risque	Document C uniquement — consignez-la avec votre raisonnement
Violation susceptible d'engendrer un risque	Document A sous 72 h + document C
Violation susceptible d'engendrer un risque ÉLEVÉ	Document A + document B dans les meilleurs délais + document C
Risque élevé, mais données incompréhensibles (chiffrées, clés en sécurité) — art 34(3)(a)	Document A + document C ; pas de document B
Risque élevé, mais des mesures ultérieures l'ont écarté — art 34(3)(b)	Document A + document C ; pas de document B
Lettres individuelles = effort disproportionné — art 34(3)(c)	Document A + communication publique + document C

L'autorité de contrôle peut ordonner la communication aux personnes concernées au titre de l'art 34(4), même lorsque vous aviez conclu qu'elle n'était pas requise. Amendes pour les manquements aux art 33/34 : jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total (art 83(4)(a)).