

Dazr Compliance · Fiche produit · Gestion des incidents

Chaque échéance d'incident, décomptée.

Enregistrez un incident et les compteurs démarrent : 72 heures pour une notification au titre de l'article 33 du RGPD, et 24 heures, 72 heures et un mois pour NIS2. Un outil fondé sur le règlement d'exécution (UE) 2024/2690 vous indique si un incident est significatif. Le registre des incidents est inclus dans tous les forfaits, Free compris.

Modifier l'incident

Enregistré le 2 oct. 2026 par `sanne.devries@brightwater.example`

Violation de données personnelles : délai RGPD de 72 heures

● Notifier l'autorité dans 17 h

Notifiez l'autorité de contrôle dans les 72 heures suivant la détection (RGPD, art. 33) : avant le 3 oct. 2026, 10:44. Le délai inclut les week-ends.

Titre

Lettre de sortie envoyée par e-mail au mauvais cabinet de r

Gravité

☐ Faible ☐ Moyenne ☒ Élevée ☐ Critique

Statut

☒ En analyse ☐ Maîtrisé ☐ Résolu ☐ Clos

Fonctionnalités clés

- ✓ **Délai RGPD** : 72 heures à compter de la connaissance de la violation pour notifier l'autorité de contrôle (Art. 33).
- ✓ **Jalons NIS2** : alerte précoce à 24 heures, notification à 72 heures, rapport final sous un mois (Art. 23).
- ✓ **Qualification des incidents significatifs** fondée sur le règlement d'exécution (UE) 2024/2690.
- ✓ **Champs de notification** demandés par une autorité, chronologie, cause racine et enseignements.
- ✓ **Portail public de signalement des violations** avec Enterprise : signalements sans compte, approuvés puis versés au registre.

Formules: Free 0 € · Basic 29 € · Pro 99 € · Enterprise 499 € par mois, HT · Custom sur demande

En savoir plus sur compliance.dazr.eu/fr/fonctionnalites/gestion-des-incidents · sales@dazr.eu · Dazr, Italie · TVA IT 02801250065**Réserver une démo**
compliance.dazr.eu

Les délais RGPD et NIS2

Chaque incident affiche un compte à rebours à partir du moment où vous en avez eu connaissance. Une violation de données personnelles déclenche le délai de l'article 33 du RGPD : 72 heures pour notifier l'autorité de contrôle, week-ends compris. Un incident NIS2 significatif déclenche les jalons de l'article 23 : une alerte précoce sous 24 heures, une notification d'incident sous 72 heures et un rapport final sous un mois. Indiquez la date d'envoi de chacun et le compteur passe au suivant.

Dazr enregistre les champs et les horodatages ; le dépôt se fait toujours sur le portail de votre autorité. Essayez le calculateur de délai de violation gratuit.

Est-ce significatif au sens de NIS2 ?

L'outil de qualification des incidents significatifs passe en revue les critères du règlement d'exécution (UE) 2024/2690 pour les entités d'infrastructure numérique et les fournisseurs numériques qu'il couvre, à partir des types d'entité et du chiffre d'affaires de votre profil de conformité. Le résultat, les critères retenus et l'heure de l'évaluation sont conservés avec l'incident, et un résultat significatif active les jalons NIS2. Un outil de qualification des incidents significatifs NIS2 gratuit est aussi disponible sur ce site.

Ce que contient une fiche d'incident

- Type (douze, de la violation de données et du rançongiciel aux incidents liés aux fournisseurs et aux incidents physiques), gravité et statut, de l'analyse à la clôture.
- Quand il s'est produit, a été détecté, contenu, éradiqué et résolu, et par qui.
- Les champs de l'article 33 : types de données concernées et nombre approximatif de personnes concernées, conséquences probables, mesures prises, contact du DPO, autorité, date de déclaration et référence du dossier, et information ou non des personnes concernées.
- Une chronologie des événements, la cause racine, l'atténuation et les enseignements, avec un lien vers une mesure corrective ou une tâche.
- Un graphique des incidents par gravité sur le registre, et le registre en exports Excel et CSV.

Un portail public de signalement des violations

Avec Enterprise, un administrateur active une page de signalement et en partage le lien. Toute personne peut signaler une violation présumée sans compte : des questions simples et l'envoi d'une capture d'écran. Une liste d'autorisation de domaines e-mail, une preuve de travail et des plafonds horaires et quotidiens bloquent le spam. Les signalements arrivent dans une file que votre responsable sécurité approuve pour les verser dans le registre des incidents, ou rejette.



Plateforme

- | | | |
|--|--|---|
| ✓ Hébergé dans l'UE, développé par Dazr en Italie | ✓ Données chiffrées au repos avec AES-256-GCM | ✓ Connexion avec Google, Microsoft ou un code par e-mail |
| ✓ Rôles : propriétaire, administrateur, membre, auditeur | ✓ Journal d'activité consultable et exportable | ✓ Anglais, néerlandais, italien, allemand, français, espagnol et polonais |

Formules: Free 0 € · Basic 29 € · Pro 99 € · Enterprise 499 € par mois, HT · Custom sur demande

En savoir plus sur compliance.dazr.eu/fr/fonctionnalites/gestion-des-incidents · sales@dazr.eu · Dazr, Italie · TVA IT 02801250065

Réserver une démo
compliance.dazr.eu