

NOTIFICATION DES FAILLES DE SÉCURITÉ

Le cadre légal

L'obligation de notifier à la CNIL les violations de données à caractère personnel est prévue à l'article 34 bis de la loi 78-17 du 6 janvier 1978 modifiée. Elle concerne uniquement les fournisseurs de services de communications électroniques au public, tels que définis par l'article L. 33-1 du code des postes et des communications électroniques (exemples : Fournisseurs d'accès à Internet, opérateurs de téléphonie fixe ou mobile).

Cette obligation sera étendue à l'ensemble des entreprises et organismes par le Règlement Européen (RGPD) applicable au 25 mai 2018, comme l'indiquent les articles 34 et 35.

Ça aurait pu être évité !

Faille de sécurité de données sensibles en ligne : Avertissement public pour le PARTI SOCIALISTE - 27 octobre 2016
Le 26 mai 2016, la CNIL a été informée de l'existence d'une faille de sécurité entraînant une fuite de données sur le site du Parti Socialiste. Lors d'un contrôle en ligne réalisé dès le lendemain, la CNIL a constaté que les mesures garantissant la sécurité et la confidentialité des données des primo-adhérents du PS étaient insuffisantes.

Source CNIL

La société ORANGE sanctionnée pour défaut de sécurité des données dans le cadre de campagnes marketing - 25 août 2014
À la suite d'une faille de sécurité concernant les données de plus d'un million de clients, la CNIL a effectué un contrôle au sein de la société ORANGE et de ses prestataires. Des lacunes de sécurité ayant été identifiées, la formation restreinte prononce un avertissement public.

Source CNIL

Comment DPMS peut vous aider ?

DPMS a développé dans PrivaCIL-DPMS un module de notification des failles de sécurité qui permet la gestion de l'information de l'autorité de contrôle. Pour chaque faille/violation identifiée, les informations sont saisies dans le formulaire du module en renseignant les huit étapes constituant la notification auprès de la CNIL (identification du responsable de traitement, type de notification, circonstances de la violation, préjudices potentiels, information des personnes concernées par la violation, etc.).

Ce formulaire est accessible aux acteurs concernés, selon leurs habilitations dans la solution (CIL/DPO, RSSI...).

Par ailleurs, une alerte est remontée sur le tableau de bord du CIL/DPO afin de lui permettre la plus grande réactivité dans le délai imparti de 72 h maximum, imposé par le RGPD.

Le workflow interne de PrivaCIL-DPMS permet d'assurer une gestion conforme des failles/violations de sécurité en respectant toutes les étapes et d'informer toutes les parties concernées.

