Une mairie victime d’un cryptovirus risque t-elle une amende de la CNIL ?

Sur le site Internet de nicematin.com on peut lire : « Cette mairie varoise victime d'une cyberattaque risque une amende de 10 millions d'euros » et encore, la liste de risques tous aussi effrayants les uns que les autres est longue. Je n'ai pas pu me retenir de réagir à ce que je considère un ramassis de bêtises.

On peut d'abord lire en tête d'article : « *Depuis jeudi dernier, la mairie de la Croix-Valmer est victime d'un virus qui crypte ses données. Et avec le renforcement de la loi protégeant les données personnelles, l'amende pourrait être salée* ».
Quelqu'un peut m'expliquer le rapport entre être victime d'un cryptovirus et RGPD ?

On peut lire un peu plus loin :
« *L'amende de la CNIL (Commission nationale de l'informatique et des libertés, NDLR) pour un défaut de sécurité concernant les données personnelles peut désormais atteindre un montant de 2% du chiffre d'affaires mondial pour une entreprise ou 10 millions d'euros maximum » nous explique Frédéric Lionetti expert cybersécurité, au cabinet Aerial.* »

Pour rappel, la victime d'un cryptovirus voit ses données chiffrées et donc devenues illisibles et inutilisables. Les données ainsi modifiées sont anonymisées, ne sont plus des données à caractère personnel et donc ne sont plus soumises au RGPD.
Comment la CNIL pourrait sanctionner un organisme en raison du fait qu'il ne dispose plus de données à caractère personnel ?
Pour un manquement à l'obligation de sécurité mentionnée dans l'article 32 du RGPD ?
Rappel Article 32 : Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:
a) la pseudonymisation et le chiffrement des données à caractère personnel;
Le RGPD conseille le chiffrement
Encore faut-il prouver qu'une personne non autorisée ou non habilitée a eu accès aux données. Dans le cas d'un cryptovirus, il ne s'agit pas d'une personne qui a pu accéder aux données mais un programme informatique (certes malveillant).

Bouquet final, l'article se termine par :
« *L'apparition d'affaires similaires pourraient se multiplier. En effet, avant la RGPD, personne n'était obligé de déclarer les attaques informatiques. Aujourd'hui, la CNIL oblige de communiquer toutes les fuites de données personnelles, comme c'est le cas depuis plusieurs années aux Etats-Unis.* »
L'attaque par cryptovirus et la fuite de données sont 2 choses différentes. Si la fuite de données n'a pas été prouvée, les victimes n'ont donc aucune déclaration de violation de données à effectuer à la CNIL.

Reste l'approche par l'impact pour les personnes concernées ?
Impossible d'apporter de service au citoyens ?
C'est le rôle des sauvegardes de pallier à cette carence et une fois de plus, si les sauvegardes n'ont pas fonctionné ou se sont aussi faîtes crypter, autant tout de suite changer d'informaticien et porter plainte contre celui qui n'a pas respecté les règles de l'art en matière de disponibilité des données. A sa place, je trouverai vite une solution pour récupérer les données et les réparer à mes frais…
A mon avis, cette Mairie ne risque rien de la part de la CNIL.
Ces avis n'engagent que moi. N'hésitez pas à réagir pour me donner votre avis.
Réagissez à cet article

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

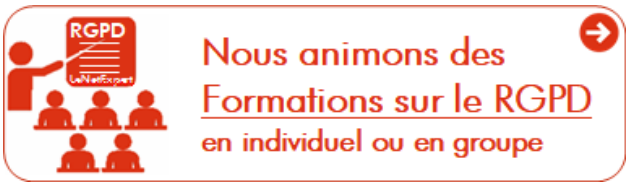
Contactez-nous

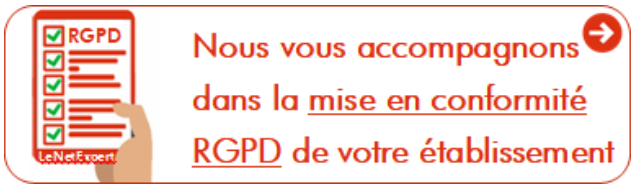
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : *Cette mairie varoise victime d’une cyberattaque risque une amende de 10 millions d’euros – Nice-Matin*