La CNIL a adopté une nouvelle recommandation ayant pour objectif de définir les exigences techniques et organisationnelles minimales pour les authentifications par mot de passe ou par tout autre secret non partagé (sauf les clés et secrets cryptographiques) mis en oeuvre dans le cadre de traitements de données à caractère personnel.

Celle-ci constitue une mise à jour de son référentiel technique destiné à apporter un niveau de sécurité minimal, en cohérence avec les bonnes pratiques de sécurité et concrètement applicable.

Il n'y a pas de caractère normatif, et ces dispositions correspondent à l'état de l'art auquel tout responsable de traitement devrait se conformer, a minima, pour satisfaire aux obligations de l'article 32 du RGPD lorsqu'il utilise une authentification par mot de passe.

D'autres mesures de sécurité peuvent être mises en place par les acteurs, si elles présentent une sécurité équivalente.

Pour aller plus loin et, notamment, déterminer les mesures nécessaires à mettre en oeuvre dans le cas où le niveau minimal décrit est insuffisant, cette recommandation sera utilement complétée par le guide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) intitulé « recommandations relatives à l'authentification multifacteur et aux mots de passe ».

Pour obtenir davantage de précisions sur cette nouvelle recommandation de la CNIL,
http://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite.

Source:

– Uroc