Commission nationale de l'informatique et des libertés

Délibération n° 2017-190 du 22 juin 2017 portant modification de la recommandation relative aux mots de passe

NOR : *CNIL1719918X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 11, 34 et 35 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe ;

Après avoir entendu M. François PELLEGRINI, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Le II. 3 de la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe dispose que :

« *S'agissant des modalités de conservation, la commission considère que le mot de passe ne doit jamais être stocké en clair. Elle recommande qu'il soit transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé.*

« La commission estime de plus que le sel ou la clé doit être généré au moyen d'un générateur de nombres pseudo-aléatoires cryptographiquement sûr (c'est-à-dire basé sur un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), et ne pas être stocké dans le même espace de stockage que l'élément de vérification du mot de passe. »

La commission décide de la suppression de ces deux alinéas qu'elle remplace par un paragraphe rédigé comme suit :

« S'agissant des modalités de conservation, la commission considère que le mot de passe ne doit jamais être stocké en clair. Elle recommande que tout mot de passe utile à la vérification de l'authentification et devant être stocké sur un serveur soit préalablement transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé. »

La présente délibération est publiée au *Journal officiel* de la République française.

Fait le 22 juin 2017.

La présidente,
I. FALQUE-PIERROTIN