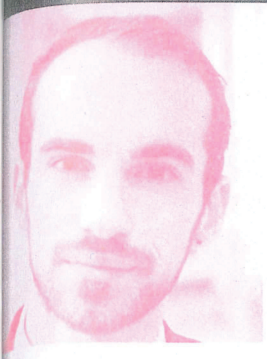
Expertises
Décembre 2015



Données personnelles Mots de passe et exigences de la Cnil

Dans une délibération du 5 novembre 2015 prononçant une sanction pécuniaire de 50 000 € à l'encontre d'Optical Center, pour manquement à l'obligation de sécurité, la Cnil vient de préciser ses attentes pour une gestion de mots de passe en conformité avec la loi Informatique et libertés.

Le principe général n'est pas nouveau : tout responsable de traitement doit prendre les mesures adéquates afin de préserver la sécurité des données qu'il traite. Derrière cette disposition résumée en quatre lignes par l'article 34 de la loi relative à l'informatique, aux fichiers et aux libertés[1], se cachent en réalité de multiples principes, plus ou moins implicites, devant être mis en œuvre par les responsables de traitements. A défaut, ces derniers sont susceptibles d'encourir des sanctions. Ainsi par sa délibération du 5 novembre dernier[2], la Cnil est venue prononcer une sanction pécuniaire à l'encontre d' « *Optical center* », célèbre lunetier, notamment en raison d'un manquement à l'obligation d'assurer la sécurité et la confidentialité des données.

Au cœur de ces enjeux de sécurité, l'un d'entre eux est récurrent : celui des mécanismes d'authentification et des règles de mots de passe. Son contour n'est pour autant pas clairement défini par les textes en vigueur. Décryptage des bonnes pratiques à adopter.

OBLIGATIONS LÉGALES EN MATIÈRE DE GESTION DES MOTS DE PASSE

Paradoxalement, les règles pratiques de gestion de mot de passe ne se trouvent pas au sein des textes législatifs. Seuls des principes généraux, sans précision pratique, peuvent s'y trouver à l'instar de l'article 34 susciter ou encore de l'article 17 de la directive européenne Informatique et libertés de 1995[3] disposant :

« *Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. [...]* »

Nous y retiendrons tout de même que **la sécurisation doit être proportionnée à la nature des données traitées ainsi qu'aux risques du traitement**, ce qui laisse une place toute singulière à une éventuelle appréciation subjective.

Pour mettre la main sur des éléments pratiques, il convient de parcourir des textes autres que législatifs ou règlementaires, tels que le « *Guide sécurité des données personnelles* » publié par la Cnil en 2010[4], les recommandations de sécurité relatives aux mots de passe de l'Anssi[5], ou encore les bonnes pratiques utilisées par les professionnels spécialisés et notamment les RSSI (Responsable de la sécurité des systèmes d'information).

Si ces recommandations et bonnes pratiques relèvent de la soft law, il n'en reste pas moins que leur respect et leur mise en œuvre sont pourtant, en pratique, contrôlés par la Cnil. Elles ne constituent pas le fondement juridique des délibérations et sanctions (c'est impossible), mais servent d'arguments pour invoquer et motiver le non-respect aux obligations générales de sécurisation.

Egalement, certaines recommandations peuvent se retrouver au sein de normes simplifiées émises par la Cnil. Ces normes sont destinées à faciliter les formalités administratives de déclaration de traitements tout en permettant d'établir des cadres types de traitements par finalités et/ou domaines d'activités. C'est ainsi qu'il est notamment possible de retrouver au sein de la norme simplifiée n°486, l'obligation pour les responsables de traitement se référant à cette norme de prévoir « *une authentification des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés [...]* ».

Il convient donc de s'intéresser à la conformité des règles de l'art mais également aux précédentes délibérations de la Cnil en matière de gestion des mots de passe afin de déterminer les attentes pratiques de l'autorité et ainsi éviter toute sanction.

RECOMMANDATIONS PRATIQUES DE GESTION DES MOTS DE PASSE

Il est nécessaire de distinguer deux types d'accès :

- d'une part les accès de responsables de traitements à leurs espaces de travail (concerne la majorité du temps les accès de salariés) ;
- d'autre part, les accès de clients aux services d'un responsable de traitement (concerne la majorité du temps les comptes clients).

Les salariés vont bien souvent avoir accès à des back-office dans lesquels un grand nombre de données à caractère personnel sont accessibles (données des bases clients, prospects, RH, etc.). Les clients vont, quant à eux, avoir accès à un simple compte personnel dans lequel leurs seules données à caractère personnel sont présentes.
Les règles de sécurité incombant à ces deux populations vont être distinctes compte tenu du niveau de risque résultant de la violation respective de l'un de ces accès.

Règles de sécurisation des mots de passe salariés

Tout responsable de traitement doit conserver à l'esprit que les règles figurant ci-dessous constituent des bonnes pratiques devant être respectées a minima. La Cnil est susceptible, en vertu du principe de proportionnalité, d'exiger des mesures de sécurisation plus poussées pour les responsables mettant notamment en œuvre des traitements de données sensibles.

Chiffrement du canal de communication

A titre d'exemple, si l'accès au back office est réalisé pour certains salariés par internet, il conviendra que la page d'authentification soit en HTTPS. Attention, tous les protocoles de transfert hypertexte sécurisés (HTTPS) ne se valent pas pour autant. En effet, certains sont considérés comme obsolètes notamment lorsqu'ils utilisent des certificats basés sur des algorithmes dépassés à l'instar du SHA-1.

Afin de sécuriser les accès distants, particulièrement développés lorsque l'entreprise dispose de chaînes de magasins physiques, d'autres mesures de sécurité peuvent être imaginées, comme par exemple la limitation de connexion à partir de certaines plages d'IP prédéfinies ou le blocage du compte salarié après X tentatives de connexion échouées.

Création de mots de passe robustes

C'est l'un des critères de non-conformité qui est régulièrement mis en avant par la Cnil dans le cadre de ses délibérations. La robustesse d'un mot de passe se définit selon différents critères parmi lesquels on retrouve notamment la taille du mot de passe, le nombre de caractères et de chiffres obligatoires qu'il doit contenir, la concordance éventuelle du mot de passe avec un mot du dictionnaire ou avec une suite de caractères fréquemment utilisée (*type azerty123456*).
C'est la combinaison de l'ensemble de ces critères qui va permettre de définir la force d'un mot de passe.
Afin de garantir l'utilisation par les salariés de mots de passe robustes, le système informatique doit imposer l'usage de mots de passe répondant à des critères prédéfinis. Un compromis doit être trouvé entre un excès de sécurité engendrant des mots de passe trop complexes à retenir et leur potentielle inscription sur des post-it volatiles par des salariés, et un zèle de sécurité sans critère minimum dans leur composition.
Un outil mis en ligne gratuitement par l'Anssi permet à tout responsable de traitement de pouvoir juger efficacement quelles règles de mots de passesaboutissent à sa robustesse : http://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/
Compte-tenu de ces différents éléments, il peut être recommandé les critères suivants :

- 12 caractères minimum,
- dont au moins 1 chiffre, 1 majuscule, 1 minuscule et 1 caractère spécial.

Néanmoins, après application de ces seuls critères, le mot de passe reste tout de même considéré comme étant faible par l'Anssi. Cela constitue pour l'Agence une taille minimale recommandée pour des mots de passe ergonomiques ou utilisés de façon locale. Afin de complexifier ce mot de passe tout en limitant sa contrainte d'utilisation par les salariés, il est recommandé de lui appliquer les critères cumulatifs suivants :

- pas plus de 3 caractères identiques ;
- interdiction d'utiliser une liste de mots prédéfinie par l'administrateur (mots du dictionnaire + suite de caractères fréquemment utilisée type azertyuiop).

Les mesures de robustesse sont considérées par la Cnil comme des mesures de sécurité élémentaires. Elle eut l'occasion de l'affirmer dans une délibération de 2014[7] prononçant une sanction pécuniaire à l'encontre de la Fédération française d'athlétisme notamment pour un manque de robustesse dans les mots de passe permettant l'accès à son système d'information.

Dans une délibération antérieure de 2013[8], elle avait par ailleurs considéré que l'utilisation de mots de passe composés pour la plupart d'une suite de cinq caractères (qui correspondaient pour certains au nom ou prénom des salariés) couplé à un non-renouvellement de ceux-ci ne permettait pas d'assurer une sécurité suffisante. Elle a à cette occasion déclaré que « *la brièveté des mots de passe, leur déductibilité, leur simplicité et l'absence de renouvellement font encourir un risque certain aux données traitées* ».

La Cnil considère par ailleurs que la mise en place de critères de robustesse de mots de passe ne présente « *pas un caractère de complexité important, [...] (qu') un simple manque de compétence ne suffit pas à justifier l'inaction de la société (en la matière)*[9] ». En effet, la Cnil ne distingue pas les responsables de traitements ayant ou non une activité liée à l'informatique et in fine, une compétence informatique : la

criticité des traitements n'était pas liée à un tel critère.

Cryptage des mots de passe contenus en base de données

A l'origine de la plainte ayant entrainé un contrôle auprès d'Optical Center, la plaignante dénonçait la communication de son mot de passe par téléphone ce qui laissait présumer un affichage en clair des mots de passe clients au sein des bases de données du lunetier.

Cette pratique est à proscrire puisqu'elle ne garantit aucune confidentialité des accès. La Cnil avait d'ailleurs pu prononcer un avertissement public en 2014 en raison de ce type d'absence de cryptage à l'encontre de la société Régime coach(10). Il convient cependant d'être vigilant sur les modes de cryptage utilisés puisque tous ne se valent pas. Ainsi, à titre d'exemple, un hachage cryptographique MD5 ne sera pas infaillible puisqu'il existe des techniques de bruteforce (tests de toutes les combinaisons possibles) ou l'utilisation de rainbow table (bases de données de MD5 et leurs équivalents en clair) qui permettront potentiellement de décrypter les mots de passe hashés contenus en base.

Imposer le renouvellement des mots de passe tous les 90 jours

Ce renouvellement doit être imposé automatiquement grâce à une configuration adaptée du système informatique. Il est très souvent mis en place sur les accès Windows (car sa configuration est particulière aisée et nativement intégrée(11)). Il reste plus rare sur les accès logiciels des salariés, car bien souvent non configurable. Il est donc essentiel de prévoir ce type de spécifications, dès la conception d'un progiciel ou dès l'acquisition de licences logiciel.

La Cnil considère ce critère comme important. Elle eut notamment l'occasion de le rappeler en énumérant des critères de non-conformité ayant conduit à prononcer une sanction pécuniaire à l'encontre de la société Loc car deam(12). Cette société imposait l'usage de mots de passe de 12 critères alphanumériques pour l'accès à l'un de ses logiciels mais n'avait prévu aucun mécanisme de renouvellement depuis sa conception.

Le renouvellement des mots de passe doit impérativement être couplé avec une historisation système des mots de passe utilisés afin d'empêcher le salarié concerné de réutiliser un mot de passe utilisé sur une période glissante d'au moins une année. Sans cette mesure, imposer un renouvellement de mot de passe peut s'avérer en pratique totalement inutile.

Mise en place d'une procédure de génération et de renouvellement des mots de passe garantissant leur confidentialité

Dans le cadre de la délibération ayant abouti au prononcé d'une sanction pécuniaire à l'encontre d'Optical center, il est notamment constaté par la Cnil que l'administrateur procédait lui-même aux renouvellements de mot de passe, en les communicant aux salariés concernés. Ce mode de fonctionnement ne permet pas de garantir la confidentialité et traçabilité des accès, et in fine l'imputabilité des actions réalisées sur ces comptes.

Afin de pallier à ces défauts de sécurité, il est recommandé :

- dans le cadre de la communication du mot de passe par un tiers ou par un système automatisé (cas typiques lorsqu'un nouveau compte est généré), d'obliger le salarié à immédiatement modifier le mot de passe communiqué. Cette obligation doit être de préférence imposée par le système informatique ;
- de permettre au salarié de pouvoir modifier directement son mot de passe ;
- de mettre par écrit la procédure appliquée au sein de la structure.

La mise en place de l'ensemble de ces règles de bonnes pratiques semble aujourd'hui indispensable. A défaut, il pourra être reproché au responsable de traitement un manque de sécurisation compromettant la confidentialité et l'intégrité des données à caractère personnel, et ce, même en l'absence de fuite de données ou d'accès non autorisé.

Il est conseillé de faire figurer l'ensemble de ces règles au sein d'une politique de gestion de mots de passe. Celle-ci peut être insérée au sein d'une charte interne d'utilisation des ressources informatiques. Mais plus important, il est surtout vivement recommandé de faire appliquer en pratique ces règles et de former les collaborateurs aux problématiques de sécurité informatique.

Il est également utile de rappeler que ces règles de mots de passe ne peuvent avoir de sens que si elles s'inscrivent dans une politique globale de sécurisation. Ainsi, un logiciel et/ou un poste inactif doit se verrouiller automatiquement passé un certain délai et cela, même si le poste est situé dans un bureau individualisé pouvant être fermé à clé.

Dans l'affaire Optical center, la Cnil a en effet considéré que les seules mesures de sécurité physique sont insuffisantes ; elles doivent impérativement être couplées à des mesures de sécurité logique.

Règles de sécurisation des mots de passe des comptes clients et prospects

Le principe de précaution devrait inciter à mettre en œuvre de règles de sécurité identiques à celles des salariés pour l'accès aux comptes de clients et/ou prospects. Cependant, ces accès sont généralement bien moins sensibles que ceux des salariés (hors cas spécifiques type banque en ligne, etc.), compte tenu du nombre limité de données accessibles depuis ces comptes. Le principe de proportionnalité doit donc trouver à s'appliquer, d'autant qu'il reste à ce jour délicat, voire contreproductif, d'imposer des règles aussi contraignantes que celles appliquées aux salariés auprès du grand public.

En toutes circonstances, les modalités de sécurisation suivantes doivent impérativement être reproduites :

- chiffrement du canal de communication ;
- cryptage des mots de passe contenus en base de données ;
- mise en place d'une procédure de génération et de renouvellement des mots de passe garantissant leur confidentialité.

Elles ne sont pas contraignantes pour le client et restent essentielles en termes de sécurisation.

La délibération Optical center vient en complément apporter un éclaircissement novateur sur les attentes de la Cnil. L'autorité administrative eut en effet l'occasion de mettre en demeure le lunetier d'améliorer la robustesse des mots de passe de ses clients.

Elle va même jusqu'à obliger cette société d'imposer à l'ensemble de ses clients le renouvellement de leurs mots de passe afin de remplir des critères de sécurité plus efficients.

En pratique, il convient donc d'imposer des critères minimum de sécurisation lorsque le client est amené à créer ou modifier le mot de passe lié à son espace client. Il est intéressant de constater que suite à la sanction, la création d'un mot de passe pour le compte-client de l'opticien est désormais conditionnée aux modalités suivantes :

- avoir au moins 8 caractères ;
- contenir au moins une majuscule ;
- contenir au moins un chiffre.

De tels critères semblent être proportionnés aux enjeux de sécurité tout en étant peu contraignants pour le client. Rappelons tout de même qu'Optical center est amené à collecter des données médicales (sur la vision et l'ouïe notamment) ainsi que des numéros de sécurité sociale pouvant se retrouver sur les espaces individuels des clients concernés. La délibération Cnil ainsi que les préconisations formulées doivent donc, en toutes circonstances, être considérées au regard du principe de proportionnalité.

Webmasters, soyez donc vigilants, la responsabilité en matière de sélection des mots de passe clients/prospects n'incombe pas ... ou du moins n'incombe plus, aux seuls utilisateurs.
Quant aux dispositifs non contraignants informant simplement l'utilisateur de la complexité du mot de passe qu'il est en train de créer ou modifier (type faible, intermédiaire, fort, très fort, etc.), ils pourraient bien ne pas suffire.

Florent GASTAUD

Juriste NTIC
Spécialiste des questions Informatique & libertés

Notes

(1) *Article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par Loi n°2004-801 du 6 août 2004. http://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006528132&cidTexte=LEGITEXT000006068624*

(2) *Délibération n° 2015-379 du 5 novembre 2015 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER : http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/2015-379_sanction_OPTICALCENTER.pdf*

(3) *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 des données à caractère personnel et à la libre circulation de ces données. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML*

(4) *Guide sécurité des données personnelles, Cnil, 2010. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf*

(5) *Agence nationale de la sécurité des systèmes d'information - No DAT-NT-001/ANSSI/SDE/NP, 5 juin 2012. http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf*

(6) *Norme simplifiée n° 48 : Délibération n° 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects. http://www.cnil.fr/documentation/deliberations/deliberation/delib/184/*

(7) *Délibération de la formation restreinte n° 2014-293 du 17 juillet 2014 prononçant une sanction pécuniaire à l'encontre de la Fédération française d'athlétisme (FFA). http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029298774&fastReqId=829990097&fastPos=1*

(8) *Délibération de la formation restreinte n°2014-261 du 26 juin 2014 prononçant un avertissement rendu public à l'encontre de la société Régime coach. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029224324&fastReqId=373570196&fastPos=1*

(9) *Délibération de la formation restreinte n°2014-307 du 17 juillet 2014 prononçant une sanction pécuniaire à l'encontre de la société Providis logistique. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029302625&fastReqId=622437988&fastPos=1*

(10) *Délibération de la formation restreinte n°2014-261 du 26 juin 2014 prononçant un avertissement rendu public à l'encontre de la société Régime Coach. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029224324&fastReqId=373570196&fastPos=1*

(11) *« Aide et astuces Microsoft » : modifier les paramètres de stratégie de mot de passe. http://windows.microsoft.com/fr-fr/windows/change-password-policy-settings#1TC=windows-7*

(12) *Délibération de la formation restreinte n° 2014-294 du 22 juillet 2014 prononçant une sanction pécuniaire publique à l'encontre de la société LOC CAR DREAM. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029298773&fastReqId=492857450&fastPos=1*