Projet de recommandation

Mots de passe

(et autres secrets non partagés)

Version soumise à consultation publique

jusqu'au 3 décembre 2021

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Sommaire

Introduction

La Commission nationale de l'informatique et des libertés (ci-après la « Commission »),

Considérant que l'utilisation d'un mot de passe est l'une des mesures de sécurisation des traitements automatisés de données à caractère personnel les plus répandue ;

Constatant que la multiplication des attaques informatiques, qui a entraîné la compromission de bases de données entières contenant notamment les mots de passe associés aux comptes des personnes concernées, a pour conséquence l'amélioration des connaissances des attaquants en matière de mots de passe ;

Relevant par ailleurs que l'emploi par les utilisateurs d'un même mot de passe pour se connecter à différents comptes en ligne, et/ou de mots de passe fondés sur des informations publiques les concernant (date de naissance, prénoms des enfants, etc.), renforce l'obligation pour les responsables de traitement de mettre en œuvre toutes mesures permettant d'assurer la sécurité des données à caractère personnel ;

Estimant nécessaire, dans l'objectif d'apporter une plus grande confiance dans les services du numérique, de définir des modalités techniques de cette méthode d'authentification à même de garantir un niveau de sécurité adapté, et d'édicter des recommandations relatives aux mesures à mettre en œuvre ainsi qu'aux règles à respecter quant à son utilisation ;

Après avoir échangé tant avec ses homologues européens qu'avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), afin de proposer une mise à jour de son référentiel technique apportant un niveau de sécurité minimal, cohérent avec les bonnes pratiques de sécurité ;

Rappelant que, dans les cas où le niveau minimal de sécurité recommandé par cette délibération est insuffisant, celle-ci sera utilement complétée par le guide de l'ANSSI intitulé « Recommandations relatives à l'authentification multifacteur et aux mots de passe », afin de déterminer les mesures de sécurité nécessaires ;

SOUMET LE TEXTE SUIVANT A CONSULTATION :

I - Recommandation générale en matière de sécurité des mots de passe

L'article 32 du RGPD impose que tout traitement de données à caractère personnel soit protégé par des mesures techniques et organisationnelles appropriées aux risques spécifiques que le traitement fait peser sur la protection des données à caractère personnel. La Commission rappelle que ces mesures doivent être déterminées de manière à garantir un niveau de sécurité adapté aux risques.

Dans ce cadre, de nombreux traitements utilisent des mots de passe ou autres secrets non partagés afin de protéger l'accès aux données qu'ils contiennent. Dans la suite du document, le terme « mot de passe » désigne tout facteur de connaissance[1], c'est-à-dire tout ensemble d'informations révocable connu uniquement de la personne concernée et permettant ou contribuant à l'authentification de celle-ci. Il inclut donc, notamment, les « phrases de passe » (réputées plus longues que les mots de passe) et les codes de déverrouillage, et exclut les clés et secrets cryptographiques.

Ce document a pour objectif de définir les exigences techniques et organisationnelles minimales recommandées par la CNIL pour les authentifications par mot de passe ou par tout autre secret non partagé (à l'exception des clés et secrets cryptographiques) mis en œuvre dans le cadre de traitements de données à caractère personnel.

En effet, d'une manière générale, la Commission recommande que tout responsable de traitement garantisse un niveau minimal de sécurité reposant, d'une part, sur une longueur et une complexité suffisantes, équivalentes à une entropie de 80 bits sans mesure complémentaire et, d'autre part, sur des règles de mise en œuvre et de gouvernance permettant de préserver la sécurité du mot de passe tout au long de son cycle de vie.

Les acteurs peuvent néanmoins mettre en œuvre d'autres mesures de sécurité que celles décrites dans cette recommandation s'ils sont en capacité de montrer qu'elles garantissent un niveau de sécurité au moins équivalent. La Commission a notamment toujours considéré que d'autres moyens d'authentification, comme par exemple l'authentification à double facteur ou les certificats électroniques, offrent davantage de sécurité que le mot de passe.

A cet égard, les risques spécifiques à certains traitements (par exemple, dans le cadre de données sensibles ou à large échelle) ou à certaines catégories d'utilisateurs (par exemple, les administrateurs informatiques) peuvent nécessiter des mesures plus rigoureuses que celles définies dans ce document, et notamment la mise en œuvre d'un processus d'authentification multi-facteurs.

II - Sur la gouvernance

La Commission recommande que tout organisme utilisant une authentification reposant sur des mots de passe définisse une politique de gestion de ceux-ci. Rédigée par les acteurs en charge de la sécurité et des moyens informatiques dans l'organisme (RSSI, DSI, DPD/DPO, par exemple), il est important qu'elle soit validée par le responsable de traitement et communiquée à toutes les personnes concernées.

Ces dernières doivent être sensibilisées aux menaces et aux risques de compromission des mots de passe, ainsi qu'au comportement à adopter en cas de suspicion de compromission de ceux-ci. Les formations doivent être adaptées aux différents publics, à leurs compétences, à leur niveau de responsabilité et à la sensibilité des données auxquelles ils ont accès. Ces formations peuvent utilement inclure un encouragement à l'utilisation de gestionnaires de mots de passe, ainsi qu'une information sur les bonnes pratiques relatives à leur utilisation (notamment sur la nécessité d'un mot de passe maître fort et la nécessité de sauvegarder régulièrement la base).

Enfin, tout dispositif mis en œuvre dans un organisme doit imposer une modification des mots de passe par défaut à la première connexion.

[1] Pour rappel, les mots de passe constituent l'un des trois facteurs possibles d'authentification définis par le guide en matière d'authentification de l'ANSSI et de la CNIL, qui sont : les facteurs de « connaissance » (détention d'une information secrète), de « possession » (détention d'un objet unique, tel qu'une carte à puce) et l'« inhérence » (caractéristique biométrique propre).

III - Sur les modalités opérationnelles de l'utilisation de mots de passe

Préambule et définitions

La Commission considère que les règles et recommandations décrites dans les annexes B1 et B2 du référentiel général de sécurité[2] (RGS) sont la référence de ce qui doit être considéré comme un « algorithme public réputé fort ». Pour assurer que « la mise en œuvre logicielle est exempte de vulnérabilité connue », la Commission recommande de ne choisir que des logiciels ou composants logiciels faisant l'objet d'une maintenance de sécurité régulière, de n'utiliser que les versions à jour de ceux-ci et d'effectuer une veille sur leur sécurité.

On appelle « entropie » la quantité de hasard contenue dans un système. Pour un mot de passe ou une clé cryptographique, cela correspond à son degré d'imprédictibilité, et donc à sa capacité de résistance à une attaque par force brute. Dans le cadre de cette recommandation, le terme d'entropie, appliqué à un mot de passe, correspond à son entropie idéale dans l'hypothèse où il serait généré aléatoirement. En informatique, on mesure couramment l'entropie en nombre de « bits », c'est-à-dire en nombre de chiffres binaires (valant soit « 0 », soit « 1 ») permettant d'exprimer la même quantité de hasard. Ainsi, un code de carte bancaire à quatre chiffres décimaux pris au hasard, valant chacun de « 0 » à « 9 », donne dix mille combinaisons possibles (10 à la puissance 4, noté 10^4). Pour obtenir un nombre de combinaisons binaires équivalent, il faut utiliser 13 bits, car 2 à la puissance 13 (ou 2^{13}) vaut 8 192, qui est du même ordre de grandeur que 10^4. On dira donc qu'un code de quatre chiffres décimaux aléatoires possède une entropie de 13 bits[3].

Toute règle de construction d'un mot de passe conduit à limiter l'espace des choix possibles, et donc à limiter son entropie pour une longueur donnée. Par exemple, choisir un mot de passe parmi les mots d'une langue revient à limiter très fortement le nombre de combinaisons de lettres possibles en pratique. En effet, chaque langue n'admet qu'un nombre limité de suites de lettres, servant à former les syllabes des mots. La tentation, pour de nombreux utilisateurs, de choisir des mots de passe « simples à retenir » facilite les attaques dites « par dictionnaire », dans lesquelles, au lieu de tester par force brute l'intégralité des combinaisons possibles, n'en sont testées qu'un nombre très limité, comprenant des mots du dictionnaire ou des prénoms, ainsi que leurs dérivations « classiques » (par exemple, du mot « kangourou », seront dérivées et testées des combinaisons telles que « k4ng0urou », « kangourou01 », « KaNgOuRoU », etc.).

De fait, lorsque les utilisateurs ont la liberté de choisir comme mot de passe des combinaisons qui ne sont pas strictement aléatoires, il est nécessaire, pour conserver un niveau d'entropie donné, de choisir une politique de mots de passe privilégiant la longueur des mots de passe par rapport à leur complexité, voire, en fonction des risques, d'augmenter le nombre de bits d'entropie cible pour la politique de mots de passe. En effet, si on s'attend à ce que les utilisateurs emploient des mots du dictionnaire, il est préférable d'imposer des mots de passe les amenant à choisir une série de mots plutôt qu'un seul. Il est recommandé de les guider dans ce choix, en leur rappelant notamment qu'il est préférable de choisir des mots qui n'ont pas de liens entre eux.

Il convient également de recommander aux utilisateurs de ne pas utiliser, pour construire leurs mots de passe, d'informations personnelles (date de naissance, prénoms des proches, etc.), ces inclusions étant à même de faciliter des attaques ciblées les concernant.

1. Modalités de l'authentification par mot de passe

Lorsque l'authentification par mot de passe s'effectue au moyen d'une connexion réseau, et a fortiori si cette dernière est opérée par un tiers, la Commission recommande :

- qu'une mesure de contrôle de l'identité du serveur d'authentification par le client soit mise en œuvre, au moyen d'un certificat d'authentification de serveur ;
- que le canal de communication entre le serveur authentifié et le client soit chiffré à l'aide d'une fonction de chiffrement sûre (c'est-à-dire mettant en œuvre un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue) ;

[2] https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

[3] Les mêmes calculs peuvent s'appliquer à des combinaisons de lettres : 26 choix possibles par caractère pour des lettres majuscules, 52 pour des lettres majuscules et minuscules, 62 si l'on ajoute les chiffres, etc.

- que des mesures de sécurité renforcées soient mises en œuvre afin de garantir la confidentialité des clés privées utilisées pour chiffrer les connexions ;
- que les mots de passe n'apparaissent pas dans les adresses des ressources distantes, ni en clair, ni sous forme hachée.

Les trois premiers points peuvent notamment être mis en œuvre par l'utilisation du protocole TLS dans une configuration respectueuse des recommandations de l'ANSSI en la matière, exposées dans son document SDE-NT-35/ANSSI/SDE/NP1 intitulé « Recommandations de sécurité relatives à TLS ».

S'agissant des modalités de création d'un mot de passe requis pour l'authentification à un compte, le responsable de traitement doit s'assurer que les mots de passe utilisés sont d'un niveau de sécurité suffisant, par exemple en imposant une taille et une complexité minimales. Elle recommande en outre que la personne ayant recours à une authentification par mot de passe soit préalablement informée de la politique mise en œuvre par le responsable de traitement, et, notamment, le cas échéant, de la taille maximale des mots de passe supportée par le traitement.

En dehors du cas des codes de déverrouillage (voir cas n° 4), la Commission recommande, dès lors que le responsable de traitement identifie un risque lié à la soumission abusive de mots de passe (notamment, si le traitement est accessible depuis Internet), de fixer une taille maximale pour les champs des mots de passe. Celle-ci doit être suffisamment grande pour permettre l'utilisation de phrases comme mots de passe, tout en évitant les attaques par déni de service résultant du traitement d'un mot de passe abusivement long. Leur taille maximale ne saurait en principe être inférieure à 50 caractères pour une authentification par mot de passe avec ou sans restriction de compte (cas n° 1 et 2). Elle pourra être, par exemple, de l'ordre de quelques centaines de caractères.

Enfin, afin d'encourager l'utilisation des gestionnaires de mots de passe et d'améliorer l'accessibilité numérique, la Commission recommande de ne pas mettre en œuvre de mécanisme ayant pour objet ou effet d'interdire aux utilisateurs de coller un mot de passe dans les champs de saisie des mots de passe, tant lors de la création du mot de passe que de l'authentification.

A l'exception des envois par voie postale, la Commission recommande que les mots de passe ne soient jamais communiqués à l'utilisateur en clair, notamment par courrier électronique. Seuls des mots de passe temporaires ou à usage unique devraient être communiqués en clair aux utilisateurs.

Dans le cas d'un envoi par voie postale, la Commission recommande l'usage de mesures complémentaires destinées à détecter son interception (p. ex. : enveloppes dont l'intérieur est noirci pour éviter la lecture par transparence, cases à gratter) ou à en empêcher l'usage (p. ex. : renouvellement forcé lors de la première utilisation du mot de passe envoyé).

Dans le cas de l'envoi de liens de création ou de renouvellement de mot de passe, il est important que les liens aient une durée d'expiration courte, d'au plus 24 heures, sauf dans le cas d'un envoi par courrier, pour lequel la durée de validité pourrait être plus longue.

Lorsqu'un mot de passe est refusé lors de sa création, un message d'information clair rappelant la politique de l'organisation en termes de mot de passe et explicitant la raison du refus doit être affiché à l'utilisateur.

La Commission estime que, dans la mesure du possible, le responsable de traitement doit conseiller et guider l'utilisateur dans la création de son mot de passe.

Elle recommande de ne pas accepter les mots de passe connus comme étant couramment utilisés. La taille et le contenu de la liste de mots de passe à refuser doivent être proportionnels aux risques et, le cas échéant, adaptés au contexte d'usage (par exemple, en incluant des listes de mots de passe interdits spécifiques au service utilisé). Dans tous les cas, l'utilisateur doit être informé que les mots de passe les plus courants ne sont pas acceptés.
Le périmètre de cette recommandation recouvrant les traitements de données à caractère personnel, la Commission considère que le niveau de sensibilité des données dont l'accès est protégé par un mot de passe ne peut pas être considéré comme faible. Dans ce contexte, et en cohérence avec les recommandations de l'ANSSI en matière d'authentification décrites dans le guide intitulé « recommandations relatives à l'authentification multifacteur et aux mots de passe », la Commission décrit quatre possibilités d'exigences minimales pour une authentification par mots de passe permettant de se conformer à cette recommandation.

Le premier cas fait reposer la sécurité principalement sur le mot de passe ; il impose par conséquent des exigences importantes en termes de niveau d'entropie, et donc de taille et de complexité du mot de passe. Dans les cas suivants, l'existence de mesures complémentaires visant à assurer un niveau de sécurité similaire permet le recours à des mots de passe d'entropie plus faible.

Cas n° 1. - Mot de passe seul

Pour se conformer à cette recommandation, si l'authentification repose uniquement sur un identifiant et un mot de passe, la Commission considère que la complexité à fixer dans la politique de mots de passe doit permettre d'assurer l'équivalent d'une entropie d'au moins 80 bits. Les trois exemples ci-dessous correspondent à cette entropie.

> Exemple 1 : les mots de passe doivent être composés d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles.
> Exemple 2 : les mots de passe doivent être composés d'au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire.
> Exemple 3 : les phrases de passe fondées sur des mots de la langue française doivent être composées d'au minimum 7 mots.

La robustesse de cette authentification reposant exclusivement sur la qualité intrinsèque du mot de passe de l'utilisateur, le responsable de traitement devra être particulièrement vigilant quant à la qualité des mots de passe de ses utilisateurs.

Cas n° 2 - Mot de passe et restriction d'accès au compte

Pour se conformer à cette recommandation, quand l'authentification prévoit un mécanisme de restriction de l'accès au compte (voir exemples ci-dessous), la complexité à fixer dans la politique de mots de passe doit permettre d'assurer l'équivalent d'une entropie d'au moins 50 bits.

> Exemple 1 : la taille du mot de passe doit être au minimum de 8 caractères et comporter 3 des 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux), les caractères spéciaux devant être pris dans un ensemble d'au moins 11 caractères ;
> Exemple 2 : les phrases de passe fondées sur des mots de la langue française doivent être composées d'au minimum 5 mots ;
> Exemple 3 : les mots de passe doivent être composés d'au minimum 15 chiffres.

L'authentification doit alors faire intervenir un mécanisme de restriction d'accès au compte. Celui-ci peut prendre une ou plusieurs des formes suivantes :

- une temporisation de l'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement en fonction du nombre de tentatives dans un laps de temps déterminé ; la Commission recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou

- un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : mise en œuvre de « captcha ») ; et/ou

- un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10, assorti d'un mécanisme de déblocage proportionnel aux risques pour les personnes d'une usurpation d'identité.

Le choix de la solution doit être opéré en prenant en compte la vraisemblance d'une attaque par déni de service, qui aurait pour objet de rendre les comptes inaccessibles, et de sa gravité pour les utilisateurs.

Cas n° 3 - Mot de passe et information complémentaire

Pour se conformer à cette recommandation, quand l'authentification comprend la fourniture d'une information complémentaire et la mise en place d'un mécanisme de restriction d'accès similaire au cas n° 2, la Commission considère que :

1) La complexité à fixer pour un tel mot de passe doit permettre d'assurer, au minimum, une entropie de 27 bits.

> Exemple 1 : la taille du mot de passe doit être au minimum de 8 chiffres décimaux ;

Exemple 2 : les mots de passe doivent être composés d'au minimum 7 chiffres hexadécimaux (chiffres décimaux et lettres de A à F, sans distinction entre majuscules et minuscules).

2) L'information complémentaire doit être communiquée en propre par le responsable de traitement ou la personne concernée. La Commission recommande alors :
   a. que cette information soit générée aléatoirement et permette d'assurer, au minimum, que l'entropie totale de l'information atteigne 23 bits :
      Exemple 1 : l'information est un identifiant de 7 chiffres décimaux générés aléatoirement ;
      Exemple 2 : l'information est composée de 6 chiffres hexadécimaux ;
   b. que celle-ci ne soit uniquement connue que de la personne et du responsable de traitement. Par conséquent, celle-ci devra être renouvelée en cas de violation de sa confidentialité ;
   c. que, si cette information correspond à l'identifiant du compte, ce dernier soit en principe exclusivement dédié à un seul service et puisse être renouvelé dans certains cas (voir section III.4) :
   d. que soit mis en œuvre une empreinte numérique de l'appareil (« *device fingerprinting* ») permettant de l'identifier, composée d'un ensemble de paramètres techniques ayant caractère d'unicité sur le terminal informatique utilisé par la personne (adresse IP, adresse MAC, type de navigateur, liste des applications installées, etc.), dont la personne a préalablement validé qu'il s'agissait d'un terminal de confiance (p. ex. : terminal non public) et qu'il peut à tout moment révoquer.

3) Une restriction de l'accès au compte doit être mise en œuvre de façon analogue au cas n° 2.

Ce cas implique la collecte d'une information complémentaire relative au terminal de l'usager. Dans une démarche de protection de la vie privée dès la conception et par défaut, ce cas ne devrait être choisi qu'après une évaluation de sa proportionnalité pour le traitement considéré.

Cas n° 4 - Code de déverrouillage

Pour se conformer à cette recommandation, quand l'authentification s'appuie sur un matériel détenu par la personne, la Commission considère que la complexité à fixer dans la politique de mots de passe doit permettre d'assurer l'équivalent d'une entropie d'au moins 13 bits.

Exemple : la taille du code personnel doit être au minimum de 4 chiffres décimaux.

L'authentification ne peut concerner qu'un dispositif matériel détenu en propre par la personne, à savoir uniquement les cartes à puce et dispositifs contenant un certificat électronique ou une paire de clés déverrouillable par mot de passe, ou tout autre mécanisme technique apportant un même niveau de sécurité.

Un blocage du dispositif doit être mis en œuvre après un nombre d'authentifications échouées consécutives au plus égal à 3.

2. Modalités de conservation

S'agissant des modalités de conservation, la Commission considère que le mot de passe ne doit jamais être stocké en clair par le responsable de traitement.

Elle recommande que tout mot de passe utile à la vérification de l'authentification soit préalablement transformé au moyen d'une fonction cryptographique spécialisée 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 un sel[4] et des paramètres relatifs aux coûts en temps et/ou en mémoire.

La Commission estime que le sel doit être généré aléatoirement et avoir en principe une longueur minimale de 128 bits. Il doit être généré pour chaque utilisateur et peut être stocké dans la même base de données.

[4] Le sel est une donnée supplémentaire qu'on ajoute aux données devant être hachées (ici, les mots de passe) afin d'empêcher que deux informations identiques donnent la même valeur hachée, sur deux systèmes informatiques différents. Utiliser un sel limite la possibilité qu'un attaquant déduise le mot de passe d'un utilisateur en regardant dans une des nombreuses bases de données de couples « mot de passe sans sel / valeur hachée » précalculés qui sont disponibles sur Internet.

Enfin, les différents éléments (taille de sel, algorithmes et paramètres) devront être régulièrement mis à jour en fonction des risques et avancées technologiques.

3. Modalités du renouvellement du mot de passe et de la notification à la personne

Pour se conformer à cette recommandation, il est nécessaire de mettre en œuvre les mesures décrites ci-dessous.

La Commission recommande que le renouvellement du mot de passe soit systématique en cas de compromission de celui-ci.

Les modalités précisées plus haut, quant à l'envoi de mots de passe à l'utilisateur par voie postale ou électronique, s'appliquent de la même façon à son renouvellement.

Renouvellement

La Commission recommande que le responsable de traitement permette à la personne concernée de procéder elle-même et de façon autonome au changement de son mot de passe. Dans ce cas, les règles afférentes à la création de mots de passe s'appliquent.

Renouvellement périodique du mot de passe

La Commission ne recommande pas que le responsable de traitement veille à imposer un renouvellement des mots de passe de l'ensemble de ses utilisateurs.

Une procédure de renouvellement périodique reste cependant nécessaire pour les comptes à privilège (comptes d'administration). Une périodicité pertinente et raisonnable sera alors à définir en fonction des risques.

Renouvellement sur demande du mot de passe par l'utilisateur

Si le renouvellement implique l'envoi d'une information (p. ex. : lien web, mot de passe temporaire communiqué par courriel ou téléphone), cet envoi doit s'effectuer via un canal préalablement validé (p. ex. : adresse courriel, moyen d'identification électronique de secours). Afin d'empêcher la compromission du mot de passe par un usage malicieux de la phase de renouvellement, il ne doit pas être possible d'envoyer le nouveau mot de passe sur un canal récemment modifié. La durée d'embargo sur les canaux récemment modifiés doit être proportionnée aux risques d'usurpation. Toute modification du canal doit être notifiée à l'utilisateur sur l'ensemble des canaux de communication validés, y compris celui ayant fait l'objet d'une modification, afin qu'il puisse être alerté si cette modification n'est pas de son fait.

Si le renouvellement fait intervenir un ou plusieurs éléments supplémentaires (numéro de téléphone, adresse postale, réponse à une question, etc.), la Commission considère que :

- les modalités permettant d'identifier que la personne demandant le renouvellement est la personne détentrice du compte ne doit pas reposer sur une réponse à une question relative à des informations habituellement publiques (p. ex. : des informations accessibles à de nombreuses personnes sur les réseaux sociaux telles que le nom des parents, le lieu d'études, le nom des animaux de compagnie, etc.) ;
- ces éléments ne doivent pas être conservés dans le même espace de stockage que l'élément de vérification du mot de passe, à moins d'être conservés sous forme chiffrée à l'aide d'un algorithme public réputé fort, et que la sécurité de la clé de chiffrement soit assurée ;
- afin de prévenir les tentatives d'usurpation s'appuyant sur le changement de ces éléments, la personne doit être immédiatement notifiée de leur modification par les moyens de communications identifiés.

La Commission recommande que la personne ait accès à une interface lui permettant de saisir un nouveau mot de passe. La validité de la session de cette interface ne doit pas excéder 24 heures, et les liens de renouvellement doivent être à usage unique.

Gestion des violations de confidentialité : notification et renouvellement

Lorsqu'une violation de son système d'information concernant un mot de passe ou des données liées à son renouvellement (p. ex. : adresse électronique) a été détectée, la Commission recommande que le responsable de traitement la notifie sans délai à la personne concernée.

Dès lors qu'il existe une suspicion de violation d'un mot de passe d'un utilisateur, la Commission estime que le responsable de traitement doit imposer à la personne concernée de le modifier lors de sa prochaine connexion,

et lui recommander de veiller à changer les mots de passe des éventuels services pour lesquels elle aurait utilisé ce même mot de passe.

Lorsqu'une information complémentaire est utilisée (cas n° 3), celle-ci doit également être renouvelée dès lors que sa confidentialité n'est plus garantie.

Enfin, concernant les données de renouvellement, les questions secrètes et leurs réponses doivent également être renouvelées en cas d'atteinte à leur confidentialité.