Analyse de la délibération de la CNIL no SAN-2022-020 du 10 novembre 2022

Lecroart, Elodie

Published in:
DPO news

Publication date:
2023

Document Version
le PDF de l'éditeur

Élodie LECROART

DPO news

Jurisprudence commentée

Analyse de la délibération de la CNIL n° SAN-2022-020 du 10 novembre 2022 : votre mot de passe est-il sécurisé et en sécurité ?

Huit cent mille (800 000) euros, c'est le montant de l'amende infligée en novembre 2022 par la formation restreinte de la CNIL[1] à la société américaine DISCORD INC. pour non-respect des principes du RGPD.

L'amende prononcée résulte du constat de l'existence de cinq manquements dans le chef du responsable du traitement. Après avoir présenté la décision dans ses grandes lignes (I), nous nous concentrerons plus particulièrement sur le manquement relatif à l'obligation d'assurer la sécurité des données conformément à l'article 32 du RGPD (II). Nous examinerons ensuite plus en détail l'obligation générale de sécurité des données et en particulier les méthodes d'authentification par mot de passe à l'aune des récentes recommandations et décisions de la CNIL (III).

I. La décision commentée

Discord est une plateforme de communication en ligne basée sur la technologie « voix sur IP » et de messagerie instantanée. La société DISCORD INC. qui édite la plateforme a été créée en 2015 et a son siège social basé à San Francisco (États-Unis)[2]. Accessible via un navigateur web ou une application, le service DISCORD permet notamment aux utilisateurs de créer des serveurs et des salons pour communiquer par écrit, en audio ou encore par vidéoconférence. La plateforme offre en outre des fonctionnalités permettant notamment le partage d'écran ou de fichiers. Principalement connu des *gamers* à son lancement, le service a progressivement bénéficié d'une audience plus large. La société annonce aujourd'hui un chiffre de 150 millions d'utilisateurs actifs chaque mois sur sa plateforme[3].

En 2020, la CNIL décide d'effectuer une mission de contrôle des traitements de données à caractère personnel effectués en ligne sur le site internet « discord.com ». À la suite des premières investigations, une commissaire-rapporteure est désignée, dont le rapport définitif est rendu en février 2022.

Sur la base de ce rapport et des observations apportées par la société DISCORD INC., cinq manquements sont retenus par la formation restreinte de la CNIL dans sa décision, à savoir :

1. **Le manquement à l'obligation de définir et de respecter une durée de conservation des données proportionnée à la finalité du traitement (art. 5.1, e), du RGPD).**

   Lors du contrôle, la formation restreinte constate que la société DISCORD INC. ne dispose pas de politique de durée de conservation des données écrite et que le registre des traitements ne mentionne aucune durée de conservation des données. En outre, la société se base sur la durée de la relation contractuelle pour conserver des comptes qui ne sont pourtant plus utilisés depuis cinq ans. Sur ce dernier point, la formation restreinte de la CNIL recommande que les comptes inactifs soient supprimés au bout de deux ans.

2. **Le manquement à l'obligation d'information des personnes (art. 13 du RGPD).**

   En lien avec le manquement précédent, la formation restreinte constate que l'information des personnes concernées sur la durée de conservation des données est formulée de manière trop générique. La formation restreinte rappelle à cet égard que l'information donnée au public concerné doit contenir soit des durées précises, soit des critères permettant de déterminer ces durées.

3. **Le manquement à l'obligation de garantir la protection des données par défaut (art. 25.2 du RGPD).**

   Par défaut, l'application DISCORD est paramétrée pour rester active même lorsque l'utilisateur ferme la fenêtre principale au moyen de l'icône « X » située en haut à droite de la fenêtre. Pour quitter l'application, l'utilisateur doit cliquer sur un autre bouton intitulé « Déconnexion ». Selon la formation restreinte de la CNIL, l'utilisateur n'est pas suffisamment informé et n'a pas forcément conscience que l'application demeure active et que ses données peuvent être communiquées à des tiers alors qu'il a cliqué sur l'icône « X ».

4. **Le manquement à l'obligation d'effectuer une analyse d'impact relative à la protection des données (art. 35 du RGPD).**

   Se référant aux lignes directrices du Groupe de travail « Article 29 »[4] établissant les critères permettant d'évaluer si une analyse d'impact est nécessaire, la formation restreinte considère que la société DISCORD aurait dû procéder à une telle analyse. Vu le nombre de données traitées et le fait que certaines données sont relatives à des enfants, le traitement doit en effet être considéré comme un traitement à grande échelle (premier critère) et relatif à des personnes vulnérables (second critère).

5. **Le manquement à l'obligation d'assurer la sécurité des données (art. 32 du RGPD).**

   Ce manquement est analysé plus en détail au point suivant (II).

[1] Commission nationale de l'informatique et des libertés, Délibération n° SAN-2022-20 du 10 novembre 2022, disponible sur www.legifrance.gouv.fr/cnil/id/CNILTEXT000046562676. À notre connaissance et au jour de la rédaction de cette contribution, la société DISCORD n'a pas manifesté son intention d'exercer un recours contre la décision. Ce recours doit en tout état de cause être intenté devant le Conseil d'État français dans les quatre mois de la notification de la décision.

[2] Ne disposant pas d'établissement dans l'UE, la société a désigné la société irlandaise VERASAFE comme représentant au sens de l'article 27 du RGPD.

[3] Selon les statistiques de la société DISCORD INC. Source : https://discord.com/company.

[4] G29, *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679*, WP 248 rev.01, modifiées et adoptées en dernier lieu le 4 octobre 2017, www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf.

Au cours de la procédure, les obligations de transparence et de respect du droit d'opposition ont également fait l'objet d'une investigation. À la suite des explications apportées par la société DISCORD, la formation restreinte de la CNIL a toutefois considéré que ces deux points n'étaient pas constitutifs de manquements.

Au moment d'évaluer les mesures correctrices à imposer à la société, la formation restreinte de la CNIL constate que les manquements avérés portent sur des obligations touchant aux principes fondamentaux de la protection des données à caractère personnel. Elle relève également que ces manquements touchent un grand nombre d'utilisateurs, dont des mineurs. En conséquence, la formation restreinte estime qu'il y a lieu de prononcer une amende administrative. Pour en déterminer le montant, l'autorité de contrôle tient compte de la nature de l'activité de la société DISCORD et de son chiffre d'affaires. La formation restreinte retient cependant la collaboration et les efforts consentis par la société DISCORD INC. au cours de la procédure pour se mettre en conformité avec ses obligations.

La CNIL décide dès lors d'infliger une amende administrative de 800 000 euros et ordonne la publicité de la décision sur son site et celui de Légifrance, mesure qu'elle justifie eu égard au nombre de personnes concernées, au nombre de manquements commis, ainsi qu'à leur gravité[5].

II. Le manquement à l'obligation d'assurer la sécurité des données (art. 32 du RGPD)

D'après le rapport soumis à la formation restreinte de la CNIL, la société DISCORD INC. manque également à son obligation en matière de sécurité des données en autorisant les utilisateurs de la plateforme DISCORD, au moment de la création d'un compte, à faire le choix d'un mot de passe constitué uniquement de six caractères incluant des lettres et des chiffres.

La commissaire-rapporteure relève que le fait d'accepter de tels mots de passe, sans exiger d'autre critère de complexité et sans adopter de mesure de sécurité complémentaire, ne permet pas d'assurer la sécurité des données et d'empêcher que des tiers non autorisés aient accès à ces données.

De son côté, la société s'est défendue en indiquant avoir mis en place des mesures permettant de garantir un niveau élevé de sécurité lors de l'accès de ses utilisateurs à son système. Elle citait notamment la limitation des tentatives de connexion à une par seconde, la vérification effectuée par e-mail ou SMS en cas de tentative de connexion provenant d'une adresse IP située en dehors de la zone de l'adresse IP de connexion précédente, le rejet des mots de passe couramment utilisés et compromis et l'implémentation d'un « captcha » pour les connexions à partir de nouvelles plages d'adresses IP.

La formation restreinte de la CNIL estime que malgré ces mesures complémentaires mises en place par la société avant la procédure, la robustesse des mots de passe admis est trop faible et conduit à un risque de compromission des comptes associés et des données à caractère personnel qu'ils contiennent. L'autorité de contrôle renvoie dans sa décision à sa *délibération n° 2017-012 du 19 janvier 2017* portant adoption d'une recommandation relative aux mots de passe dans laquelle elle détaille les modalités techniques qui doivent être mises en œuvre lorsque des responsables du traitement ont recours à un mécanisme d'authentification par mot de passe.

Dans cette recommandation, la CNIL considère que lorsque l'authentification prévoit un mécanisme de restriction de l'accès au compte[7], le mot de passe doit comporter au minimum huit caractères, contenant au moins trois des quatre catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux).

Dans le cadre de la procédure, la société DISCORD a renforcé ses processus de sécurité des mots de passe en instaurant deux nouvelles mesures :

1. l'exigence d'un mot de passe d'une longueur minimale de huit caractères, dont au moins trois sont des lettres minuscules, des lettres majuscules, des chiffres ou des caractères spéciaux ;
2. la résolution d'un « captcha » après dix tentatives de connexion infructueuses.

Bien que la société se soit mise en conformité au cours de la procédure, la formation restreinte de la CNIL estime que le manquement à l'article 32 du RGPD est établi dès lors que l'ancienne politique de gestion des mots de passe de la société n'était pas suffisamment robuste et contraignante pour garantir la sécurité des données et entraînait un risque pour les personnes concernées.

III. L'obligation de sécurité des données : les méthodes d'authentification par mot de passe à l'aune des récentes recommandations et (autres) décisions de la CNIL

A. L'obligation de sécuriser les données (art. 32 du RGPD)

La sécurisation des systèmes d'information et des données qu'ils contiennent est un enjeu majeur de la réglementation relative à la protection des données à caractère personnel, ainsi que d'un certain nombre d'autres réglementations générales[8] ou particulières[9].

Le point commun de ces réglementations est qu'elles imposent de se fonder sur une approche par les risques pour déterminer les mesures techniques et organisationnelles à mettre en œuvre afin de garantir un niveau de sécurité qui soit adapté au risque existant.

Ainsi, l'article 32 du RGPD impose que le choix des mesures de sécurité tienne compte de plusieurs facteurs tels que l'état des connaissances, les coûts de mise en œuvre des mesures, la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, leur degré de probabilité et leur niveau de gravité. Les mesures de sécurité doivent donc être adoptées au regard des caractéristiques du traitement et aux risques que celui-ci engendre pour

[5] Notons que la mesure de publicité prévoit que la société ne sera plus nommément identifiée à l'expiration d'un délai de deux ans à compter de la publication de la décision.

[6] Disponible sur www.legifrance.gouv.fr/jorf/id/JORFTEXT000033928007. Cette délibération a toutefois été abrogée par la Délibération n° 2022-100 du 21 juillet 2022 (voy. ci-après).

[7] La CNIL cite des exemples de tels mécanismes : la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (comme un « captcha ») et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses.

[8] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), *J.O.U.E.*, n° L 333 du 27 décembre 2022, p. 80.

[9] Voy. par exemple le règlement (UE) n° 2014/910 sur les services de confiance ou la directive (UE) 2015/2366 relative aux services de paiement dans le marché intérieur.

les personnes concernées, et être proportionnées au niveau de risque identifié.

Cette obligation doit notamment être lue en parallèle avec l'article 5.1, f), du RGPD qui énonce que les données doivent être traitées de manière sécurisée au moyen de mesures techniques et organisationnelles qui les protègent contre toute forme de traitement illicite ou non autorisé, et contre la perte, la destruction ou encore les dégâts d'origine accidentelle. En d'autres termes, ces mesures doivent garantir l'intégrité et la confidentialité des données.

Il découle de cette obligation que le responsable du traitement (ou le sous-traitant) doit d'une part procéder à une identification préalable des risques inhérents au traitement en vue de définir le niveau de risque global et les types de mesures à adopter. Pour ce faire, le responsable du traitement doit procéder ou faire procéder à des audits de sécurité périodiques et, si nécessaire, à une analyse d'impact conformément à l'article 35 du RGPD. D'autre part, le responsable du traitement doit également mettre en place une procédure visant à tester régulièrement l'efficacité des mesures prises pour garantir le caractère approprié dans le temps des mesures.

Le premier paragraphe de l'article 32 du RGPD énonce des exemples de mesures pouvant être implémentées en fonction des besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Tant la doctrine[10] que les autorités de contrôle n'ont pas manqué de détailler ces procédures et moyens concrets permettant d'atteindre un niveau de sécurité adapté au risque. Nous renvoyons ainsi le lecteur au *Guide* de la CNIL sur la sécurité des données personnelles[11] qui fournit des fiches pratiques et détaillées pour évaluer le niveau de sécurité des données à caractère personnel d'un organisme et adopter les précautions élémentaires pour préserver la sécurité des données.

Le tableau tel que repris à la fin de la contribution constitue une synthèse de ces moyens et procédures recommandés par la CNIL.

B. Les recommandations de la CNIL relatives aux mots de passe et autres méthodes d'authentification

Dans le cadre de la décision commentée, la CNIL renvoie à sa délibération n° 2017-012 du 19 janvier 2017 dans laquelle elle édicte des recommandations relatives aux mots de passe dont aurait dû tenir compte la plateforme en ligne DISCORD.

En juillet 2022, la CNIL a justement mis à jour ses recommandations en adoptant une *nouvelle délibération n° 2022-100*[12]. Celle délibération abroge et remplace donc la délibération précitée du 19 janvier 2017.

Partant du constat que les attaquants en matière de mots de passe sont de plus en plus performants, et que les personnes concernées ont parfois tendance à utiliser un même mot de passe pour différents comptes en ligne et/ou des mots de passe fondés sur des informations publiques les concernant, la CNIL entend par ces recommandations renforcer les exigences techniques et organisationnelles minimales applicables aux méthodes d'authentification par mot de passe.

C'est également l'occasion pour la CNIL de rappeler que les traitements impliquant des risques spécifiques, par exemple parce qu'ils concernent des données particulières et/ou constituent des traitements à grande échelle de données, nécessiteront la mise en œuvre de mesures plus contraignantes comme par exemple un processus d'authentification multifacteur. La Commission cite notamment le cas d'un service de messagerie électronique comme faisant partie de ces traitements à risques plus élevés.

Concrètement, la CNIL définit trois types de scénarios dans lesquels le mot de passe est utilisé, seul ou en combinaison avec d'autres mesures, comme méthode d'authentification. Pour chacun de ces cas, elle identifie le niveau d'exigence minimale applicable au choix de ce mot de passe en tenant compte d'une mesure appelée « entropie »[13] qui correspond au degré d'imprédictibilité d'un mot de passe ou encore à sa capacité à résister à une attaque par force brute.

> À titre d'exemple, lorsqu'il est utilisé seul, un mot de passe doit, selon la CNIL, être composé d'au moins douze caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux ou d'au moins quatorze caractères s'il ne comprend pas de caractères spéciaux obligatoires.
>
> La taille du mot de passe pourra toutefois se limiter à huit caractères comprenant au moins trois catégories parmi les quatre précitées (majuscules, minuscules, chiffres et caractères spéciaux) si le mot de passe est combiné à un mécanisme de restriction d'accès au compte tel que la limitation du nombre maximal de tentatives autorisées dans un délai donné.

Dans la mesure où les utilisateurs ont tendance à employer des mots du dictionnaire, la CNIL invite en tout état de cause à privilégier la longueur des mots de passe (série de mots qui n'ont, de préférence, pas de lien entre eux) par

[10] Voy. notamment C. Charlier et J. Vigneron, « Développement informatique et sécurisation technique des données personnelles », *in* A. Beelen et N. Ragheno (coord.), *La protection des données et les entreprises. Défis, opportunités et impact du RGPD sur les départements clés de l'entreprise*, Limal, Anthemis, 2022, pp. 157 et s.

[11] Disponible sur www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf.

[12] CNIL, Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n° 2017-012 du 19 janvier 2017, disponible sur www.cnil.fr/sites/default/files/atoms/files/deliberation-2022-100-du-21-juillet-2022_recommandation-aux-mots-de-passe.pdf.

[13] Définition du Larousse : « Dans la théorie de la communication, nombre qui mesure l'incertitude de la nature d'un message donné à partir de celui qui le précède. (L'entropie est nulle lorsqu'il n'existe pas d'incertitude) ».

rapport à leur complexité. Elle rappelle également que l'usage d'informations personnelles (prénoms, dates de naissance de proches…) est strictement déconseillé.

L'autorité de contrôle française attire encore l'attention des responsables du traitement sur l'importance de ne pas stocker les mots de passe en clair mais bien de les transformer préalablement au moyen d'une fonction cryptographique spécialisée et intégrant un « sel », à savoir une donnée supplémentaire générée de manière aléatoire et ajoutée au mot de passe préalablement à son hachage.

Bien que cela puisse surprendre, la CNIL ne recommande plus d'imposer à l'ensemble des utilisateurs (excepté en ce qui concerne les comptes à privilèges) une modification périodique du mot de passe. En effet, l'imposition d'une telle mesure pousse en général les utilisateurs à ne modifier que très légèrement leurs mots de passe successifs et à choisir des mots de passe peu robustes (avec des critères d'identification personnels tels que date de naissance ou autres…) pour faciliter leur mémorisation.

Notons encore que les activités liées à l'authentification des utilisateurs et à la gestion de leurs mots de passe doivent faire l'objet d'une journalisation.

Enfin, en cas d'atteinte ou de suspicion d'atteinte à la confidentialité d'un mot de passe, l'utilisateur concerné doit être informé et doit être en mesure de modifier son mot de passe.

Cette recommandation ne préjudicie en rien l'avis de la CNIL selon lequel d'autres moyens d'authentification tels que l'authentification à double facteur ou les certificats électroniques, offrent davantage de sécurité que le seul mot de passe. En outre, la CNIL considère que les mesures définies dans cette *recommandation doivent être complétées par les Recommandations relatives à l'authentification multifacteur et aux mots de passe* publiées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[14].

C. Autres décisions récentes de la CNIL en matière de sécurité liée aux mots de passe

Plusieurs décisions récentes faisant état de manquements à l'obligation de sécurité des données concernaient la politique de gestion des mots de passe mis en œuvre par les responsables du traitement impliqués. En voici un bref aperçu :

- **Délibération de la formation restreinte n° SAN-2022-018 du 8 septembre 2022 concernant le GIE INFOGREFFE**[15]

  Le site web « infogreffe.fr » permettait aux utilisateurs titulaires des 3,7 millions de comptes de se connecter à partir d'un mot de passe limité à huit caractères maximum, sans critère de complexité et sans mesure de sécurité complémentaire.

  Dans sa décision, la formation restreinte considère que le défaut de robustesse du mot de passe expose les utilisateurs à un risque réel, à savoir celui qu'un tiers non autorisé identifie le mot de passe et accède à toutes les données à caractère personnel présentes dans le compte de la personne concernée.

  Ce risque se concrétise notamment par le fait que l'organisme INFOGREFFE transmet en clair par courrier électronique les mots de passe, lesquels ne sont pas temporaires ni à usage unique et dont le renouvellement n'est pas imposé. En outre, l'utilisateur ne reçoit pas de confirmation en cas de modification du mot de passe et n'est dons pas protégé contre les tentatives d'usurpation de son compte.

  La CNIL rappelle également dans cette affaire que la caractérisation d'un manquement à l'article 32 du RGPD ne nécessite pas l'existence réelle d'une violation de données mais peut être le résultat de mesures jugées insuffisantes pour garantir la sécurité des données traitées[16].

  Une amende de 250 000 euros est dès lors infligée à INFOGREFFE pour manquement aux obligations contenues aux articles 5.1, e), et 32 du RGPD.

- **Délibération de la formation restreinte n° SAN-2022-021 du 24 novembre 2022 concernant la société ÉLECTRICITÉ DE FRANCE**[17]

  Dans cette décision, EDF, principal fournisseur d'électricité en France, s'est vu imposer une amende de 600 000 euros pour divers manquements, dont celui d'assurer la sécurité des mots de passe des utilisateurs.

  Il est reproché à la société de conserver les mots de passe d'accès à l'espace client de plus de 25 000 comptes de manière non sécurisée avec une fonction de hachage MD5. Or, cette fonction est considérée depuis 2004 par la CNIL comme non robuste et présentant des vulnérabilités connues. L'utilisation de cette fonction permettrait notamment à un tiers ayant connaissance du mot de passe haché de déchiffrer facilement celui-ci[18].

  La formation restreinte constate également que les mots de passe sont uniquement hachés, sans avoir été salés, c'est-à-dire sans que des caractères aléatoires aient été ajoutés avant le hachage, ce qui est pourtant recommandé par l'ANSSI.

- **Délibération de la formation restreinte n° SAN-2022-022 du 30 novembre 2022 concernant la société FREE**[19]

  Dans cette affaire, l'opérateur de téléphonie fixe écope d'une amende de 300 000 euros.

  La formation restreinte relève notamment que les mots de passe générés aléatoirement lors de la création d'un compte ne sont pas assez robustes. De plus, ces mots de passe sont transmis aux utilisateurs en clair, par courrier postal ou courrier électronique, sans qu'ils soient temporaires ni que la société impose d'en changer. Enfin, ces mots de passe sont stockés en clair dans la base de données de la société.

  Toujours concernant la sécurité, mais cette fois-ci plus en lien avec la politique de gestion des mots de passe, l'autorité de contrôle constate que les mesures techniques et organisationnelles appliquées lors du reconditionnement des boîtiers « freebox » d'anciens

[14] Disponibles sur www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/.

[15] Disponible sur www.legifrance.gouv.fr/cnil/id/CNILTEXT000046280956?init=true&page=1&query=san-2022-018&searchField=ALL&tab_selection=all.

[16] Point 39 de la décision.

[17] Disponible sur www.legifrance.gouv.fr/cnil/id/CNILTEXT000046650733?isSuggest=true.

[18] Point 64 de la décision.

[19] Disponible sur www.legifrance.gouv.fr/cnil/id/CNILTEXT000046693390?init=true&page=1&query=san-2022-022&searchField=ALL&tab_selection=all.

abonnés n'ont pas permis d'empêcher que ces boîtiers soient attribués à de nouveaux clients alors que des données (dont des photos et vidéos personnelles) relatives aux anciens abonnés n'avaient pas été correctement effacées.

Conclusion

Mesure technique et organisationnelle parmi d'autres, la mise en place d'un mécanisme d'authentification par mot de passe nécessite de la part du responsable du traitement qui y recourt une évaluation sérieuse et préalable des risques que fait peser le traitement sur les personnes concernées.

La décision commentée permet d'insister sur l'importance de définir une politique de gestion de ces mots de passe qui soit adaptée au cas d'espèce, à charge pour le responsable du traitement d'en assurer la publicité et la mise en œuvre auprès des utilisateurs de ses services ainsi que de procéder à des révisions régulières de celle-ci.

Bien que les recommandations de la CNIL en la matière n'aient pas un caractère normatif, elles correspondent, selon l'autorité de contrôle française, « 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 mots de passe pour protéger un traitement »[20].

En 2021, le *Data Breach Investigation Report* de la société Verizon avait identifié que 81 % des violations de données étaient causées par des mots de passe compromis, faibles, ou réutilisés[21].

Élodie Lecroart

Avocate au barreau de Namur

[20] Point 5 de la délibération n° 2022-100.

[21] https://linc.cnil.fr/fr/de-azerty-paword-une-revue-des-pratiques-de-gestion-des-mots-de-passe.

Tableau récapitulatif des moyens et procédures à mettre en œuvre pour assurer la sécurité des données au sens de l'article 32 du RGPD

Évaluer le niveau de sécurité des données personnelles de votre organisme

Avez-vous pensé à ?

Fiches		Mesures	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	□
		Rédigez une charte informatique et lui donner une force contraignante	□
2	Authentifier les utilisateurs	Définissez un identifiant (*login*) unique à chaque utilisateur	□
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	□
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	□
		Limitez le nombre de tentatives d'accès à un compte	□
3	Gérer les habilitations	Définissez des profils d'habilitation	□
		Supprimez les permissions d'accès obsolètes	□
		Réalisez une revue annuelle des habilitations	□
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	□
		Informez les utilisateurs de la mise en place du système de journalisation	□
		Protégez les équipements de journalisation et les informations journalisées	□
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	□
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	□
		Utilisez des antivirus régulièrement mis à jour	□
		Installez un « pare-feu » (*firewall*) logiciel	□
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	□

6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	□
		Faites des sauvegardes ou synchronisations régulières des données	□
		Exigez un secret pour le déverrouillage des smartphones	□
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	□
		Sécurisez les accès distants des appareils informatiques nomades par VPN	□
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	□
8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	□
		Installez sans délai les mises à jour critiques	□
		Assurez une disponibilité des données	□
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	□
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	□
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	□
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	□
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	□
		Stockez les supports de sauvegarde dans un endroit sûr	□
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	□
		Prévoyez et testez régulièrement la continuité d'activité	□
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	□
		Détruisez les archives obsolètes de manière sécurisée	□
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	□
		Encadrez par un responsable de l'organisme les interventions par des tiers	□
		Effacez les données de tout matériel avant sa mise au rebut	□
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	□
		Prévoyez les conditions de restitution et de destruction des données	□
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	□
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	□
		Assurez-vous qu'il s'agit du bon destinataire	□
		Transmettez le secret lors d'un envoi distinct et via un canal différent	□
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	□
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	□
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	□
		Évitez les zones de commentaires ou encadrez-les strictement	□
		Testez sur des données fictives ou anonymisées	□
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	□
		Conservez les secrets et les clés cryptographiques de manière sécurisée	□

Source : www.cnil.fr/sites/default/files/atoms/files/check_list_0.pdf