

LE COFFRE-FORT NUMÉRIQUE : UNE MEILLEURE SÉCURISATION DE VOS DOCUMENTS

Fiche pratique J 334

Date de publication : 27/12/2018 - Internet/multimédia



Le coffre-fort numérique permet d'archiver des documents sur des serveurs distants et accessibles par internet (également appelé « cloud »). Les documents sont stockés dans un espace sécurisé et confidentiel, et sont accessibles à tout moment.

A partir du 1^{er} janvier 2019, les fournisseurs de services de coffre-fort numérique devront renforcer la sécurité des services ainsi que l'accès à l'information.

Cette fiche pratique vous donne des conseils pour choisir et bien utiliser votre coffre-fort numérique.

- 1 - [Qu'est-ce qu'un coffre-fort numérique ?](#)
- 2 - [Quelles informations fournir à l'utilisateur avant l'ouverture d'un compte ?](#)
- 3 - [Quelles informations doivent obligatoirement figurer au contrat ?](#)
- 4 - [Comment s'assurer de l'exclusivité d'accès à vos données ?](#)
- 5 - [Quelles mesures de sécurité et de confidentialité doivent être prises par le fournisseur du service ?](#)
- 6 - [Quelles mesures de traçabilité doivent être prises par le fournisseur du service ?](#)
- 7 - [Comment s'organise la récupération des documents ?](#)
- 8 - [Quelles informations donner à l'utilisateur en cas de fermeture du compte ?](#)
- 9 - [Existe-t-il des certifications et des labels ?](#)
- 10 - [Conseils avant d'ouvrir un compte sur un service de coffre-fort numérique](#)

1 - Qu'est-ce qu'un coffre-fort numérique ?

L'article L.103 du code des postes et des communications électroniques établit la définition légale d'un service de coffre-fort numérique dont il décrit l'objet et les critères de fonctionnement.

Jusqu'ici la notion de coffre-fort numérique était imprécise. Elle permettait à certains fournisseurs de service de proposer des services de stockage peu sécurisés. La CNIL relève que les utilisateurs de ces services pouvaient être induits en erreur par des services de stockage qui ne constituent pas un coffre-fort numérique, car ne présentant pas les mêmes garanties de confidentialité des données ([délibération n° 2017-178 du 1^{er} juin 2017](#)).

A compter du 1^{er} janvier 2019, les services de coffre-fort numérique répondront à des règles strictes. Deux décrets viennent compléter l'article L. 103 du code des postes et des communications électroniques et, définir la notion de coffre-fort numérique. Leur date d'entrée en vigueur est le 1^{er} janvier 2019 :

- [le décret n°2018-418 du 30 mai 2018](#) relatif aux modalités de mise en œuvre du service de coffre-fort numérique,
- [le décret n°2018-853 du 5 octobre 2018](#) relatif aux conditions de récupération des documents et données stockées par un service de coffre-fort numérique.

BON A SAVOIR : Les dispositions applicables au coffre-fort numérique sont codifiées à l'article L. 103 du Code des postes et des communications électroniques.

Cet article est issu de [l'article 87](#) de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique et de [l'article 1^{er}](#) de l'ordonnance n°2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques.

2 - Quelles informations fournir à l'utilisateur avant l'ouverture d'un compte ?

Avant que l'utilisateur ne crée un compte en utilisant un service de coffre-fort numérique, le fournisseur du service doit lui fournir une information claire, loyale et transparente sur les modalités de fonctionnement et d'utilisation du service ([article R. 55-1](#) du Code des postes et des communications).

Le fournisseur du service doit communiquer à l'utilisateur, de manière lisible et compréhensible, les informations suivantes :

- le type d'espace mis à sa disposition et les conditions d'utilisation associés,
- les mécanismes techniques utilisés,
- la politique de confidentialité,
- l'existence et les modalités de mise en œuvre des garanties de bon fonctionnement,

- l'engagement du fournisseur du service sur la conformité des services aux exigences fixées aux [1° à 5° de l'article L. 103](#) du Code des postes et des communications électroniques. Un dossier technique, devant être tenu par le fournisseur du service, permet de démontrer le respect de ces exigences. Ces informations sont également mises à disposition en ligne et, le cas échéant, mises à jour.

IMPORTANT Vous bénéficiez également de la réglementation applicable à la vente à distance (durée, coût, délai de rétractation, médiateur de la consommation, etc.).

> Pour en savoir plus, lire la fiche INC "[Acheter sur Internet en 10 questions-réponses](#)".

3 - Quelles informations doivent obligatoirement figurer au contrat ?

Avant que l'utilisateur ne crée un compte sur un service de coffre-fort numérique, le fournisseur du service doit préalablement lui fournir un contrat.

Ce contrat doit comporter les éléments suivants ([article D. 539](#) du code des postes et des communications électroniques) :

- les modalités de récupération des documents (opérations techniques que doit conduire l'utilisateur, caractéristiques techniques du format du fichier, délai de récupération),
- les conditions dans lesquelles le format d'un document déposé dans le service pourrait être transformé par le fournisseur du service,
- les frais éventuels exigibles en cas de demandes de récupération excessives de l'utilisateur.

A NOTER : L'utilisateur doit consentir de manière expresse à ces informations qui doivent être mises en ligne de façon aisément accessible (ex. consentement par le biais d'une case à cocher aux CGV comprenant les informations obligatoires).

4 - Comment s'assurer de l'exclusivité d'accès à vos données ?

Le fournisseur du service doit garantir, à l'utilisateur, un "accès exclusif" du service. L'utilisateur peut également, après avoir donné son **autorisation explicite**, permettre à des tiers d'accéder à ses documents (ex : conjoint de l'utilisateur, etc.) ([article L. 1034°](#) du code des postes et des communications électroniques).

La garantie d'un accès exclusif requière au minimum la mise en œuvre des mesures suivantes :

- un mécanisme de contrôle d'accès limitant l'ouverture du coffre-fort numérique aux seules personnes autorisées par l'utilisateur,
- des mesures de sécurité destinées à garantir la confidentialité des documents et données stockés ainsi que des métadonnées (*) correspondantes,
- le chiffrement par le service de coffre-fort numérique de l'ensemble des documents et données lors de leurs stockages, transferts vers ou depuis le service. Ce chiffrement doit être effectué à l'aide de mécanismes cryptographiques conformes à l'état de l'art et permettre une évolution de la taille des clés et des algorithmes utilisés ([article R. 55-6](#) du code des postes et des communications électroniques).

(*) informations qui permettent de décrire les différents aspects d'une donnée, en lui donnant un contexte (ex. document Excel : taille du fichier, date de création, titre, commentaires, etc.).

A NOTER : La conformité à l'état de l'art est présumée lorsque les mécanismes impliqués dans ces opérations de chiffrement sont conformes aux [règles et recommandations de l'Agence nationale de sécurité des systèmes d'information \(ANSSI\)](#) concernant le choix et le dimensionnement des mécanismes cryptographiques.

5 - Quelles mesures de sécurité et de confidentialité doivent être prises par le fournisseur du service ?

Le fournisseur du service doit assurer que l'intégrité, la disponibilité et l'exactitude des données et documents stockés dans le coffre-fort numérique sont garanties par des mesures de sécurité adaptées et conformes à l'état de l'art ([article R. 55-3](#) du code des postes et des communications électroniques).

L'identification de l'utilisateur doit être assurée par un moyen d'identification électronique adaptée aux enjeux de sécurité du service ([article R. 55-5](#) du code des postes et des communications électroniques).

6 - Quelles mesures de traçabilité doivent être prises par le fournisseur du service ?

La traçabilité des opérations réalisées sur les données et documents stockés dans le coffre-fort numérique et la disponibilité de cette traçabilité pour l'utilisateur requièrent au minimum la mise en œuvre des mesures suivantes :

- l'enregistrement et l'horodatage des accès et tentative d'accès,
- l'enregistrement des opérations affectant le contenu ou l'organisation des données et documents de l'utilisateur,
- l'enregistrement des opérations de maintenance affectant les données et documents stockés dans les coffres-forts numériques.

A NOTER : Les durées de conservation des données de traçabilité constituent une mention obligatoire du contrat de fourniture de service de coffre-fort numérique ([article R. 55-4](#) du code des postes et des communications électroniques).

7 - Comment s'organise la récupération des documents ?

1 - L'utilisateur a le droit de récupérer ses documents et données, **à tout moment, et à titre gratuit. Il n'existe pas de restriction sur le nombre d'opérations de récupération.**

Si les demandes de récupération de l'utilisateur sont excessives (ex : demandes ayant un caractère abusivement répétitif), le fournisseur du service peut dans ce cas :

- exiger le paiement de frais raisonnables qui tiennent compte des coûts supportés pour organiser la récupération des documents et données demandées,
- refuser de donner suite à ces demandes ([article D. 540](#) du code des postes et des communications électroniques).

2 - L'utilisateur du service peut récupérer ses documents et données :

- par voie de communication électronique, et par une requête, de façon simple et sans manipulation complexe ou répétitive,
- dans un format électronique ouvert, structuré, couramment utilisé, aisément réutilisable et exploitable par un système de traitement automatisé. Sauf dans le cas des documents initialement déposés dans un format non ouvert, qui peuvent être restitués dans leur format d'origine.

L'opération de récupération doit s'effectuer de façon complète, intégrée et dans un délai raisonnable.

Seules doivent être collectées les données confidentielles ou les données à caractère personnel de l'utilisateur, qui sont indispensables à la bonne exécution de l'opération de recrutement ([article D. 537](#) du code des postes et des communications électroniques).

A NOTER : Les dispositifs de récupération doivent assurer un niveau d'intégrité et de confidentialité des documents et données au moins équivalent à celui des fonctions permettant la réception, le stockage, la suppression et la transmission des données ([article D. 538](#) du code des postes et des communications électroniques).

8 - Quelles informations donner à l'utilisateur en cas de fermeture du compte ?

L'utilisateur doit être informé **au mois 3 mois à l'avance** de la suspension ou de la fermeture du service afin qu'il puisse récupérer les documents et données stockés dans son coffre-fort numérique.

Que faire en cas d'absence d'information préalable sur la suspension ou la fermeture du service, ou lorsque, l'utilisateur cesse durablement d'être en mesure d'accéder aux services et ce qu'elle qu'en soit la raison ?

Le fournisseur du service doit garantir la récupération des documents et données pendant une durée de **12 mois** à compter de la date à laquelle cette cessation d'activité au service est intervenue ([article D. 541](#) du code des postes et des communications électroniques).

9 - Existe-t-il des certifications et des labels ?

Les services de coffre-fort numérique peuvent bénéficier d'une certification établie selon un cahier des charges proposé par l'autorité nationale des systèmes d'information (ANSSI) après avis de la Commission Nationale de l'Informatique et des Libertés (CNIL) et approuvé par arrêté du ministre chargé du numérique ([article L. 103](#) du code des postes et des communications électroniques).

NOTRE CONSEIL : Privilégier les services de coffre-fort numérique certifiés, gage de sécurisation et de confidentialité des données (certification en cours d'élaboration). En attendant la certification élaborée par la CNIL et l'ANSSI, les labels suivants sont à privilégier :

- [norme française NF Z42-020 de l'AFNOR](#) "Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps",
- [norme internationale ISO 14641 : 2018](#) "Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intégrée de documents électroniques – Spécifications".

A NOTER : L'hébergement des données de santé dispose d'un régime spécifique. Il est conditionné par l'obtention d'un agrément ministériel spécifique. La CNIL relève que les fournisseurs de services de coffre-fort numérique qui n'auraient pas été agréés à héberger des données de santé devraient être tenus de déconseiller à leurs utilisateurs de stocker des données relatives à la santé ([délibération n° 2017-178 du 1^{er} juin 2017](#)).

10 - Conseils avant d'ouvrir un compte sur un service de coffre-fort numérique

1 - Privilégiez les services de coffre-fort numérique certifiés ou disposant d'un label, permettant de vous garantir une sécurisation et une confidentialité de vos données.

2 - Lisez attentivement les conditions générales et la politique de protection des données personnelles du service auquel vous souhaitez souscrire. Notamment les points concernant :

- l'accès **exclusif** à vos données,
- le lieu de stockage des serveurs,
- les mesures de sécurité, de confidentialité et de traçabilité des données,
- la portabilité des données,
- la récupération de vos données,
- l'utilisation commerciale ou non des données.

3 - Veillez à stocker vos données de santé uniquement dans les coffres-forts numériques agréés par un agrément ministériel spécifique. Ce sont des services de coffre-fort numériques très sécurisés destinés à recevoir des données sensibles telles que les données de santé.

Samia M'HAMDI
Juriste à l'Institut national de la consommation