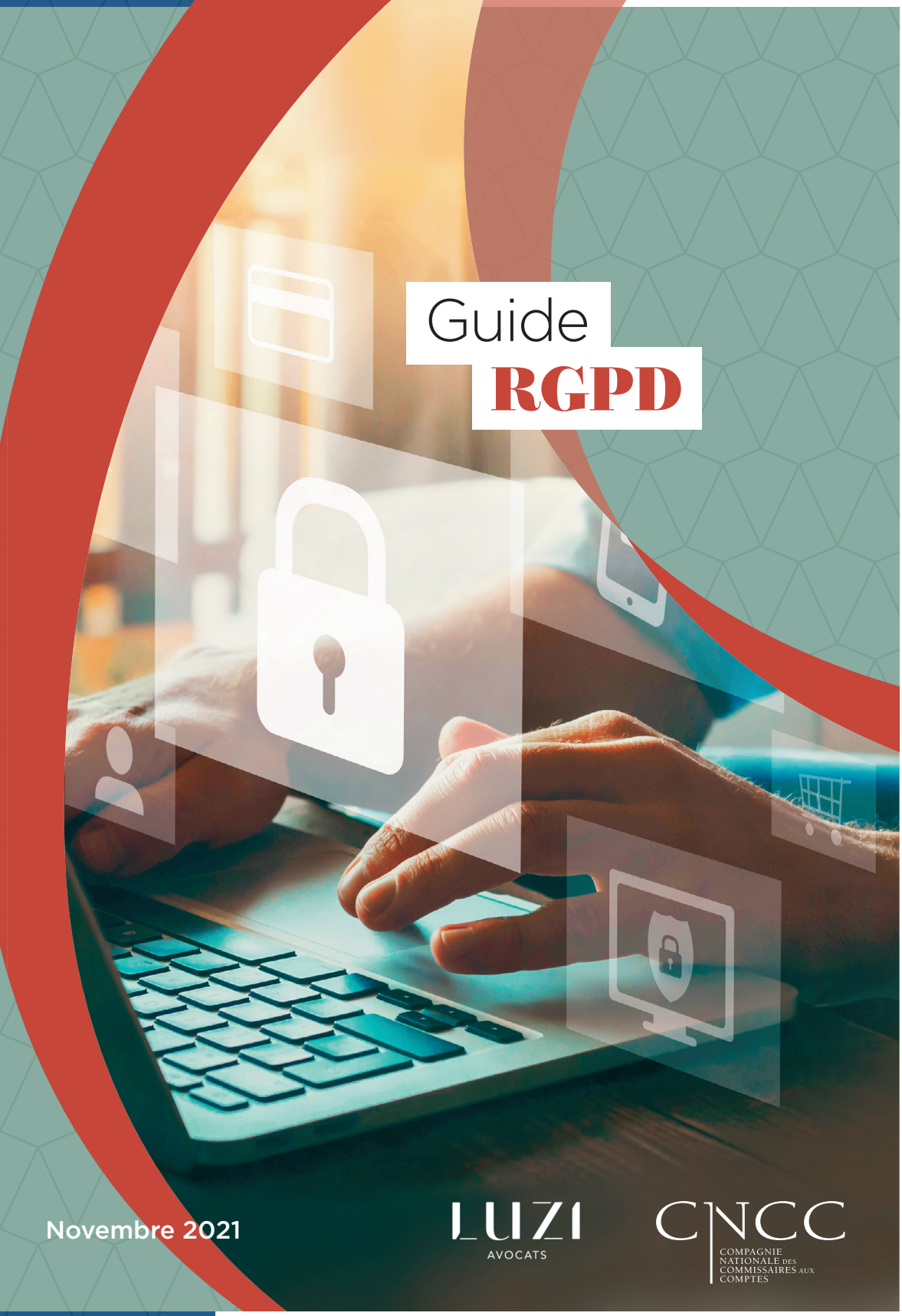
Guide RGPD



Novembre 2021

LUZI AVOCATS

CNCC COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Préface

Publié sous l'égide de la Compagnie nationale des commissaires aux comptes, ce guide a été conçu et élaboré par un groupe de travail composé de délégués à la protection des données personnelles, de commissaires aux comptes, juristes et avocats, accompagnés par le Cabinet Luzi Avocats, spécialisé en droit du numérique et en droit de la vie privée et des données personnelles.

Quelle que soit votre structure d'exercice, vous êtes amenés en tant que commissaire aux comptes à collecter, analyser et conserver des données personnelles confiées par les entités contrôlées. Votre conformité à la règlementation est un travail continu et constitue un gage de transparence et de confiance pour l'ensemble des acteurs du marché.

Ce guide a vocation à aider la profession des commissaires aux comptes à se conformer à la règlementation applicable en matière de protection des données à caractère personnel ; il aborde la protection des données sous l'angle de l'exercice, par le commissaire aux comptes, de ses missions et prestations. Il n'a pas vocation à aborder la protection des données traitées à des fins de gestion des cabinets (gestion des ressources humaines par exemple), pour laquelle vous pouvez vous référer aux publications et à la doctrine de la CNIL.

Ce guide est composé de **dix fiches pratiques** destinées à répondre aux interrogations que vous pouvez vous poser en matière de protection des données personnelles dans l'exercice de votre profession :

Fiche n° 1 – Gouvernance et « *Accountability* » : Cette fiche, introductive, rappelle les grands principes et explique aux commissaires aux comptes la manière dont ils peuvent documenter leur conformité, notamment à l'aide d'une documentation *« data privacy »*. La fiche pratique propose, en annexe, un modèle de fiche de registre des activités de traitements incluant les traitements identifiés comme propres à l'activité de commissaire aux comptes.

Fiche n° 2 – Le statut du commissaire aux comptes : Cette fiche expose (i) les raisons pour lesquelles il faut considérer que le commissaire aux comptes est responsable des traitements effectués dans le cadre de ses missions (certification des comptes, SACC, etc.), ainsi que (ii) des recommandations quant à la gestion de ses rapports avec d'autres acteurs (experts, entités contrôlées, etc.) notamment sur la question de l'information des personnes concernées. À ce titre, la fiche propose en annexe un modèle de courrier d'information à destination des clients (entités contrôlées) du commissaire aux comptes.

Fiche n° 3 – Gestion de la relation professionnelle (clients et prospects) : Cette fiche énonce les bonnes pratiques et écueils à éviter tout au long du cycle de vie de la relation professionnelle qu'entretiennent les commissaires aux comptes avec les entités contrôlées (ses clients et prospects). Nous abordons les mentions d'information, les bonnes pratiques associées à l'usage d'outils de gestion de la relation client (CRM). Un point de vigilance est mis en avant concernant la procédure de KYC *(Know Your Client)*, avec en annexe un modèle de fiche de registre de traitement spécifique au traitement KYC.

Fiche n° 4 – Transparence – Information : Cette fiche a pour objet de guider le commissaire aux comptes dans la mise en oeuvre de son obligation d'information en tant que responsable du traitement (collecte directe et indirecte de données personnelles) et des dérogations envisageables.

Fiche n° 5 – Gestion des droits RGPD : Cette fiche a pour objet de guider le commissaire aux comptes dans sa gestion pratique des demandes d'exercice de droits des personnes concernées : données concernées, documents communicables, modalités de réponse, délais et limitations opposables à ces demandes d'exercice de droits, etc.

Fiche n° 6 – Le RGPD dans un contexte Co-CAC : Cette fiche a pour objet de clarifier les statuts et rôles respectifs des cabinets de commissariat aux comptes qui sont nommés dans une mission de co-commissariat aux comptes. Dans ce contexte, chaque cabinet intervient de manière indépendante. Plus particulièrement cette fiche propose de guider les commissaires aux comptes en cas d'incident de sécurité entrainant, le cas échéant, une violation de données personnelles.

Fiche n° 7 – Transferts hors UE – mise en place de garanties appropriées : Cette fiche a pour objet de guider les commissaires aux comptes en cas de transferts internationaux de données personnelles en proposant une méthodologie des actions à mettre en place pour assurer un niveau de protection adéquate dans le cadre de ces transferts. Sont également présentés au sein de cette fiche, à l'aide de cas pratiques, les mécanismes proposés par le RGPD (BCR, clauses contractuelles types, certification, etc.) appliqués à l'activité de commissariat aux comptes. Est annexé à la fiche le modèle de clauses contractuelles types approuvées par la Commission Européenne. Cette fiche aborde également la question de l'encadrement des transferts de données personnelles hors de l'Union Européenne à la suite de l'invalidation par la Cour de justice de l'union européenne du mécanisme du *Privacy Shield* dans l'arrêt dit Schrems II du 16 juillet 2020.

Fiche n° 8 – Sécurité des données : Cette fiche rappelle les règles essentielles à appliquer en matière de sécurité ainsi qu'une synthèse des principales mesures de sécurité recommandées par la CNIL.

Fiche n° 9 – Contrôle et sanctions CNIL : Cette fiche présente les grandes étapes d'un contrôle et les sanctions encourues. Par ailleurs, la fiche a pour objectif de présenter aux commissaires aux comptes leurs droits et obligations ainsi qu'une méthodologie organisationnelle afin de faciliter la conduite des opérations de contrôle réalisées par la CNIL.

Fiche n° 10 – Gestion de la sous-traitance : Cette fiche a pour objet de guider le commissaire aux comptes dans la gestion de ses relations contractuelles avec ses sous-traitants au sens du RGPD (personnes physiques et/ou morales traitant les données à caractère personnel pour son compte). La fiche énonce les bonnes pratiques à mettre en place afin d'identifier les traitements concernés (catégories de données concernées, localisation des données, connaître son sous-traitant, etc.), ainsi qu'une méthodologie permettant au commissaire aux comptes de définir et communiquer ses instructions (un modèle est proposé à titre d'exemple en annexe).

Nous espérons que ce guide vous aidera dans la mise en place de bonnes pratiques en la matière !

Bonne lecture,

Yannick OLLIVIER,
Président de la Compagnie nationale des commissaires aux comptes

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Avant-propos

Après trois ans d'application du règlement général sur la protection des données personnelles (RGPD), **l'Europe est en passe de gagner son pari** d'offrir une véritable opportunité pour les citoyens européens, mais aussi les entreprises et les États membres de l'UE, de regagner leur place dans le numérique, avec un contrôle et une maîtrise accrue des données les concernant. Cet outil s'inscrit dans la stratégie de reconquête de souveraineté numérique, de réduction de la dépendance actuelle vis-à-vis des géants mondiaux.

Pourtant, le RGPD fait peur. On ne peut nier qu'il soit complexe. Il concerne tous les secteurs d'activité, publics et privés, toutes les entreprises quelle que soit leur taille. Si la prise de conscience croissante que les données, et tout particulièrement **les données personnelles, constituent un actif stratégique pour l'entreprise**, les mesures à prendre peinent parfois à être identifiées, implémentées et suivies dans le temps. Il est vrai que cela nécessite de connaitre les systèmes d'information et le « qui fait quoi » en matière de données. L'application concrète des principes de proportionnalité et de minimisation, le respect des droits des personnes (droit à l'information, droit d'opposition ou de consentir dans certains cas…), les mesures techniques et organisationnelles appropriées afin d'assurer la sécurité et la fixation de durées de conservation suscitent souvent de nombreuses questions.

C'est la raison pour laquelle **ce nouveau guide RGPD**, fait par et pour les commissaires aux comptes avec le concours d'un cabinet d'avocat, représente un atout indéniable. Il présente en effet un intérêt double :

- **Sur le plan opérationnel, la présentation en dix fiches pratiques permet d'identifier les 10 réflexes à avoir pour assurer sa conformité au RGPD, conformément au principe de « responsabilisation » du professionnel qui doit être en mesure de pouvoir démontrer qu'il est conforme à la réglementation.**

Il ne s'agit pas d'un guide figé dans le temps car il concerne une matière vivante. Ainsi, en matière de transferts de données personnelles hors UE dans la mesure où les modèles de clauses contractuelles types approuvées par la Commission Européenne sont évolutives, les dispositions du guide sont susceptibles d'ajustements.

- **Sur le plan pédagogique, ce guide assure la diffusion d'une culture de « protection des données personnelles » adaptée aux missions et traitements mis en oeuvre par la profession sous l'angle de l'exercice de sa mission.**

La diffusion de cette culture chez tous les responsables de traitements publics comme privés est un impératif pour le succès du RGPD. Or, il s'avère qu'elle repose avant tout sur la volonté des dirigeants, seuls capables d'impulser la dynamique pour sensibiliser les équipes et organiser la conformité de manière dynamique, tout au long du cycle de vie de la donnée, au sein de leur entreprise et avec l'ensemble de leurs partenaires et sous-traitants.

Détenteur d'une mission d'intérêt général et en tant que vecteur de confiance, le commissaire aux comptes doit s'en approprier les enjeux et s'investir dans sa propre conformité.

La profession entend répondre aux problématiques nouvelles du numérique qui sont aussi des opportunités, ainsi qu'en témoigne son rapport d'activité : comment mesurer le coût d'une non-conformité au RGPD alors que les risques cyber explosent ? comment traduire l'information extra financière ou une RSE adaptée à de petites entités, dont fait partie la bonne gouvernance des données prévue par le RGPD.

Ce guide constitue donc la brique initiale et peut être complété par les **outils réutilisables conçus par la CNIL** (MOOC, logiciel pour faire les analyses d'impacts, guides multiples dont celui sur la sensibilisation des TPE PME co-édité avec BPI France, autoévaluation de maturité en gestion de la protection des données…) adaptés aux spécificités des commissaires aux comptes.

Sophie NERBONNE

Directrice chargée de la co-régulation économique – CNIL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Avant-propos

Sommaire général

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Gouvernance & *Accountability*

Gouvernance & *Accountability*

Fiche n° 1

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

Le principe d'*accountability* implique :

1. l'obligation de **traiter les données personnelles dans le respect des principes fondamentaux** de la protection des données (licéité, loyauté et transparence du traitement, minimisation des données, etc.) ;
2. l'obligation d'**être en mesure de démontrer à tout moment sa conformité** à la Règlementation applicable.

Ce qui constitue un travail continu au sein de votre cabinet.

Votre cabinet doit **se munir d'une documentation « *data privacy* »** à jour comprenant *a minima :*

1. Un **registre des activités de traitement** de données à caractère personnel,

   Dans la mesure où vous traitez des données personnelles de manière régulière, **vous êtes obligé de tenir un registre des activités de traitement** et ce quel que soit le nombre de salariés dans votre cabinet, y compris si vous exercez l'activité de commissaire aux comptes en travailleur indépendant.

2. Des **mentions d'information types** sur les traitements réalisés, qui doivent figurer dans vos lettres de mission, et idéalement.
3. Une **politique de confidentialité.**

Cette documentation a notamment vocation à être présentée aux agents de la CNIL en cas de contrôle et à démontrer votre conformité à la Réglementation applicable.

Le **RGPD** et la **loi informatique et liberté** renforcent les droits des personnes concernées et créent de nouvelles obligations à la charge des responsables du traitement et des sous-traitants.

En particulier, la Règlementation applicable met fin au régime de déclaration simplifiée et instaure un principe d'*accountability* **(1)** dont la mise en œuvre doit être appréhendée tant au sein du cabinet qu'à l'égard des tiers **(2)**.

Comme tout responsable du traitement, les cabinets de commissaires aux comptes[1] sont tenus de documenter les actions mises en place pour se conformer au RGPD, notamment à l'aide d'un registre des activités de traitement **(3).**

[1] Dans le cas d'un exercice au sein d'un cabinet de commissariat aux comptes, le responsable de traitement est le cabinet en tant que personne morale et non le commissaire aux comptes salarié du cabinet.

Gouvernance & *Accountability*

Sommaire

1. Définition et teneur du principe d'*accountability*

La CNIL définit l'*accountability* comme « *l'obligation pour les entreprises de mettre en œuvre* ***des mécanismes et des procédures internes permettant de démontrer*** *le respect des règles relatives à la protection des données* »[2].

Le principe d'*accountability* signifie que tout organisme mettant en œuvre un traitement de données à caractère personnel doit être capable de démontrer le respect des **principes définis à l'article 6 § 1 du RGPD**, à savoir les principes de :

- **Licéité :** le traitement doit reposer sur l'une des six bases juridiques énoncées à l'article 6 § 1 du RGPD[3]. Généralement, les traitements mis en œuvre par les commissaires aux comptes auront pour base légale le respect d'une obligation légale ou l'intérêt légitime poursuivi par le commissaire aux comptes, responsable du traitement (Cf. Fiches de la Cnil : « L'obligation légale : dans quels cas fonder un traitement sur cette base légale ? », « L'intérêt légitime : comment fonder un traitement sur cette base légale ? »)

Par exemple : le traitement consistant en l'archivage des dossiers par le commissaire aux comptes pendant une durée minimum de 6 ans a pour base légale le respect de l'obligation légale prévue à l'article R. 821-68 du Code de commerce.

- **Loyauté** et **transparence** : les personnes concernées doivent être informées du traitement et des droits dont elles disposent sur leurs données.

Par exemple : vos conditions d'intervention et votre lettre de mission doivent contenir un article relatif aux données personnelles prévoyant notamment les modalités d'information des personnes concernées (cette information doit être assurée par l'entité contrôlée, Cf. Fiche n° 4 du guide « Transparence – Information »).

- **Limitation des finalités :** les données doivent être collectées pour une finalité explicite, légitime et déterminée.

Par exemple : Le traitement mis en œuvre par le commissaire aux comptes dans le cadre d'une mission d'audit a pour finalité la certification des comptes sociaux et consolidés. Il s'agit d'une finalité légitime et déterminée. En revanche, si ces mêmes données sont utilisées à des fins étrangères à la mission du commissaire aux comptes, il s'agira d'un détournement de finalité.

[2] https://www.cnil.fr/fr/definition/accountability

[3] **Article 6 § 1 du RGPD :** *« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : **a)** la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités, **b)** le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; **c)** le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; **d)** le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; **e)** le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; **f)** le traitement est nécessaire aux intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel notamment lorsque la personne concernée est un enfant ».*

- **Minimisation** et **exactitude** des données collectées : Seules les données adéquates et pertinentes au regard de la finalité du traitement doivent être collectées. Ces données doivent être exactes, et si nécessaire, mises à jour.

Par exemple : En cas de changement de dirigeant de l'entité contrôlée en cours de mission, le commissaire aux comptes doit mettre à jour les données qu'il détient sur le dirigeant de cette entreprise. De même, le commissaire aux comptes ne doit conserver dans son dossier que les données personnelles utiles et nécessaires à la documentation de ses diligences. (À titre d'exemple, lors du traitement des provisions pour congés payés, le commissaire aux comptes doit inviter l'entité contrôlée à ne pas lui fournir de données superflues, telles que le numéro de sécurité sociale des employés, leurs coordonnées bancaires…).

- **Limitation de la conservation :** Les données personnelles ne peuvent être conservées que pour une durée limitée à ce qui est nécessaire au regard des finalités pour lesquelles elles ont été collectées.

Par exemple : Les dossiers de travail du commissaire aux comptes doivent être conservés pendant une période de 6 ans[4]. Les cabinets peuvent conserver ces dossiers de travail pendant plus longtemps pour une durée additionnelle en considération des durées de prescriptions légales.

- **Intégrité et confidentialité :** Les données doivent être traitées dans des conditions garantissant un niveau de sécurité et de protection adéquat contre les risques de violation de données (Vous pouvez notamment vous référer aux recommandations figurant dans le guide sécurité de la CNIL[5] dans sa dernière version en vigueur, aux 10 Commandements de la cybersécurité publiés par la CNCC, ainsi qu'à la Fiche n° 8 du guide *« Sécurité des données »*, qui présentent quelques exemples des bonnes pratiques à mettre en œuvre en la matière).

Par exemple : assurez-vous que les mots de passe d'accès de vos collaborateurs sont suffisamment robustes (Cf. Commandement n° 1 *« La confidentialité tu garantiras »*[6]) et que des antivirus et des pare-feux sont mis en place (Cf. Commandement n° 2 *« De boucliers tu te muniras »*[7]). Si les messageries des membres de votre cabinet sont stockées sur le cloud, assurez-vous que les données demeurent dans l'UE (Cf. Fiche RGPD de la CNCC n° 2 *« Sensibilisez vos équipes »*[8]). Il est également recommandé de vous munir d'une politique de gestion

[4] **Article R. 821-68 du Code de commerce :** *« Les dossiers et documents établis par le commissaire aux comptes en application de l'article R. 823-10 sont conservés pendant six ans, même après la cessation des fonctions. Ils sont, pour les besoins des contrôles et des enquêtes, tenus à la disposition des autorités de contrôle, qui peuvent requérir du commissaire aux comptes les explications et les justifications qu'elles estiment nécessaires concernant ces pièces et les opérations qui doivent y être mentionnées ».*

[5] https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

[6] **Commandement n° 1 :** *« Renforcez la politique de gestion des mots de passe : utilisez des mots de passe robustes (minimum 8 caractères, mots n'existant pas dans le dictionnaire, utilisation de caractères spéciaux et de chiffres) différents pour chaque accès et renouvelez-les tous les 3 ou 4 mois ».*

[7] **Commandement n° 2, voir les rubriques** *« Munissez-vous d'antivirus et d'antispam » et « Disposez de pare-feux actifs ».*

[8] **Fiche RGPD de la CNCC n° 2 :** *« Partagez ces principes de précautions. Veillez à utiliser des services de cloud garantissant que les données demeurent dans la zone de l'UE. Sinon, assurez-vous que les mesures requises par le RGPD sont mises en œuvre ».*

des violations de données afin d'anticiper ces situations et de gérer ce type d'incidents (Cf. Fiche n° 8 du guide *« Sécurité des données »* et Fiche de la CNIL « *Les violations de données »*[9]).

*À noter : L'*accountability *implique pour votre cabinet deux obligations : (1) celle de traiter les données dans le respect des principes mentionnés ci-dessus (mise en place de mesures, de procédures, etc.) et (2) celle de pouvoir justifier à tout moment de votre conformité (trace documentaire de la mise en œuvre de ces mesures)*[10]*. Sans documentation, votre cabinet pourrait être considéré non conforme au principe d'*accountability.

2. La mise en œuvre du principe d'*accountability*

2.1 L'*accountability* au sein du cabinet

Le respect du principe d'*accountability* constitue un moyen pour le cabinet de vérifier sa propre conformité. Cela requiert la mise en place d'un **programme de conformité continu couvrant tout le cycle de vie des données** destiné à :

- **Superviser l'utilisation des données personnelles tout au long de l'activité de votre cabinet**. Au besoin, un comité *ad hoc* peut être créé au sein de votre cabinet pour gérer les problématiques en matière de protection des données personnelles.
- **Évaluer votre profil de risque en fonction de votre activité.** Une approche par le risque consiste pour votre cabinet à évaluer le degré de probabilité et de gravité du risque pour les droits et libertés des personnes en fonction notamment de la finalité des traitements mis en œuvre et de la nature des données. Il s'agit d'identifier les traitements présentant des risques pour les individus et notamment de déterminer si une analyse d'impact est nécessaire. Au besoin, un logiciel open source est mis à votre disposition par la CNIL pour vous accompagner dans la réalisation d'analyses d'impact[11].
- **Détecter au fur et à mesure les non-conformités et points à améliorer.** La conformité à la Règlementation applicable s'inscrit dans un processus d'amélioration continue **il y aura toujours des points à améliorer et à corriger** tout au long de l'activité de votre cabinet.

Par exemple : En mettant à jour la liste de vos sous-traitants au sens du RGPD (ex. éditeurs de logiciels SaaS de tenue de comptabilité, hébergeurs, traducteurs, etc.), vous vous rendez compte que le contrat conclu avec ces derniers ne comporte pas toujours de dispositions relatives au traitement des données personnelles. Vous devez corriger cette non-conformité

[9] *« Il est dès lors recommandé que les organismes qui traitent des données personnelles (responsable du traitement ou sous-traitant) prévoient et mettent en place des procédures globales en matière de violation de données personnelles ».*
[10] **Article 24.1 du RGPD** *« le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer* ***et*** *être en mesure de démontrer que le traitement est effectué conformément aux présent règlement ».*
[11] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

en proposant à votre sous-traitant un avenant permettant d'encadrer les traitements qu'il réalise pour votre compte dans le respect de la Règlementation applicable.

- **Mettre en place en interne des politiques et procédures** relatives à la protection des données et en assurer le suivi effectif[12]. Ces politiques et procédures doivent être maintenues et mises à jour tout au long du traitement (Cf. Commandement n° 6 *« Le RGPD tu respecteras »*[13]) et être adaptées en considération de la nature des données traitées.

Par exemple : Dans le cadre de certaines de ses missions, le commissaire aux comptes peut être amené à connaitre de données sensibles (déclarations annuelles d'emplois des travailleurs handicapés (DOETH), litige pénal impliquant une personne physique, accidents du travail…). Le traitement de ces données sensibles[14] doit faire l'objet d'une attention particulière (accès à ces données restreints, mesures de sécurité renforcées…).

- **Former et sensibiliser les salariés** impliqués dans la collecte et le traitement de données à caractère personnel. Les salariés amenés à traiter des données doivent être sensibilisés aux mesures de sécurité, à la confidentialité des données et aux principes du RGPD.

Par exemple : Il est essentiel pour votre cabinet de se munir d'une Charte informatique prévoyant les règles fondamentales que tout salarié doit respecter en matière de sécurité informatique (Cf. Commandement n° 9 *« Les usages tu règlementeras »*[15], Cf. Fiche de la Cnil *« Sécurité : sensibiliser les utilisateurs »*)

À noter : L'accountability est **un concept dynamique** visant à améliorer votre conformité de manière constante. L'*accountability* peut également constituer **un gage de confiance** pour vos clients (Cf. Fiche RGPD n° 1 CNCC *« Quatre bonnes raisons de se mettre en conformité avec le RGPD »*[16]).

2.2 L'*accountability* à l'égard des tiers

À l'égard des tiers, l'*accountability* s'entend comme l'obligation pour votre cabinet de justifier de sa conformité auprès de la CNIL en cas de contrôle.

[12] **Article 24.2 du RGPD** « Les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement ».

[13] **Commandement n° 6 :** *« Étape 5 : Mettez en place des procédures internes pour assurer la protection des données tout au long du traitement ».*

[14] Les données sensibles font partie des catégories particulières de données personnelles définies à l'article 9 du RGPD comme des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Fiche RGPD de la CNCC n° 2 : *« Action #3 Structurez votre démarche : Intégrer ces principes de précaution dans la charte informatique de votre cabinet et faites-la signer à l'ensemble de vos équipes. Partagez avec vos équipes au moins une fois par an sur ces sujets ».*

[15] **Commandement n° 9 :** *« Encadrer les pratiques par l'utilisation d'une charte informatique. La mise en place d'une charte informatique est indispensable… voire obligatoire dès lors que le cabinet collecte des données à caractère personnel ».*

[16] **Fiche RGPD de la CNCC n° 1 :** *« Avantage #2 : Renforcez la confiance avec vos clients. En vous positionnant comme acteur de la confiance numérique, parce que vous protégez les données à caractère personnel que vous êtes susceptible de traiter dans le cadre de vos missions, vous vous inscrivez dans une dynamique vertueuse et positive ».*

Comme tout responsable du traitement, les commissaires aux comptes doivent pouvoir démontrer à tout moment leur conformité. **Cela implique de se ménager une preuve de sa conformité en se constituant une documentation.**

> *À noter :* Il est essentiel de documenter votre conformité afin de pouvoir démontrer que la protection des données est une préoccupation constante au sein du cabinet. (Cf. Fiche RGPD de la CNCC n° 6 *« Documentez votre démarche »*[17], Cf. Fiche de la CNIL *« Documenter la conformité »*).

La documentation de votre conformité sert d'état des lieux précis des actions mises en place par votre cabinet et doit couvrir tant les aspects organisationnels que contractuels et techniques.

Elle est notamment composée des documents suivants :

Documents de type « organisationnel » :

- Le registre des traitements [18] (Cf. Modèle fourni en annexe de la présente fiche).
- Le registre des violations de données (Cf. Fiche n° 8 du guide *« Sécurité des données »*).
- Les éventuelles analyses d'impact qui ont été menées (Cf. Fiche de la CNIL sur l'AIPD).
- La politique de sécurité/Charte informatique du cabinet.
- Plus généralement toute politique/procédure interne destinée à assurer le respect de la Règlementation applicable (politique de durées de conservation des données, de gestion des demandes d'exercice de droit d'accès, procédure de gestion des violations de données …).
- La cartographie des traitements mis en œuvre (Cf. Fiche RGPD de la CNCC n° 4 *« Réalisez une cartographie des données collectées et de leurs traitements »*[19]).
- La liste tenue à jour de l'ensemble de vos sous-traitants (fournisseurs de services cloud, éditeurs de logiciels de gestion, hébergeurs…).

Documents de type « contractuel » :

- Modèle de lettre de mission indiquant que le commissaire aux comptes agit en qualité de responsable du traitement (Cf. Lettres de mission CNCC et Fiche n° 2 du Guide relative au *« Statut du commissaire aux comptes »*).
- Politique de protection des données mise à la disposition des entités contrôlées.

[17] **Fiche RGPD de la CNCC n° 6 :** *« Action #2 : Documentez l'ensemble des opérations et procédures dédiées à la protection des données pour démontrer votre mise en conformité (…) Cette documentation est d'autant plus importante à réaliser que le nouveau règlement s'accompagne d'un renversement de la preuve : en cas de contrôle, c'est à l'entreprise de démontrer qu'elle est conforme à la règlementation ».*

[18] Le registre des activités de traitement est obligatoire (Article 30 du RGPD : *« Chaque responsable du traitement, et le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité »*).

[19] **Fiche RGPD de la CNCC n° 4 :** *« Action #1 : Formalisez une cartographie » et « Action #2 : Organisez sa mise à jour. Cette cartographie présente l'avantage de vous donner une vision précise de la nature des données collectées. Donc d'identifier celles qui méritent une vigilance accrue dont découleront les actions de mise en conformité correspondantes ».*

- Clause encadrant la sous-traitance, afin de démontrer que vous exigez de vos sous-traitants le même niveau de confidentialité que celui que vous garantissez aux entités contrôlées (Cf. Fiche RGPD de la CNCC n° 5 « Sécurisez vos relations avec vos prestataires »[20], Cf. Exemple de clauses de sous-traitance de la CNIL).
- Clauses contractuelles types approuvées par la Commission Européenne, règles d'entreprises contraignantes (en particulier, lorsque votre cabinet appartient à un réseau de cabinets d'audit dans le monde et que des transferts internationaux de données ont lieu entre eux) et tout autre dispositif encadrant des transferts de données conformément à la Règlementation applicable (Cf. Fiche de la CNIL *« Transférer des données hors de l'UE »* et Fiche de la CNIL *« Les règles d'entreprise contraignantes »*).

Documents de type « technique » :

- Rapport(s) d'audit(s) de conformité à la Règlementation applicable.
- Certifications ISO 27001 et déclarations d'applicabilité (le cas échéant).
- Liste des mesures techniques mises en place pour protéger les données personnelles traitées.

De manière générale, il faut considérer que le respect des obligations qui vous incombent en tant que responsable du traitement doit faire l'objet d'une documentation pouvant être fournie à tout moment en cas de contrôle de la CNIL.

Comment assurer la bonne tenue de cette documentation ?

Il est recommandé de désigner une personne au sein du cabinet chargée en tant que référent de piloter la conformité et de gérer la documentation de votre conformité (Cf. Fiche RGPD de la CNCC n° 3 *« Dynamisez votre cabinet, désignez un référent »*[21]). Selon la taille de votre cabinet, il pourra s'agir d'un comité *ad hoc* se réunissant régulièrement pour suivre les problématiques de protection des données dans votre cabinet.

Par exemple : Le comité *ad hoc* peut vérifier si l'usage de nouvelles technologies au sein de votre cabinet nécessite de réviser les dispositions des conditions générales d'intervention de votre cabinet ou la politique de confidentialité.

À noter : Ce référent ou ce comité *ad hoc* en charge des problématiques de protection des données ou le délégué à la protection des données (« DPO »), quand il en a été désigné un, a vocation à se coordonner avec les différentes parties prenantes qui traitent des données personnelles (notamment celles des entitées controlées) et contribuer à la conformité du cabinet dans son ensemble.

Pour plus d'information sur la nécessité de désigner un DPO et la fonction de DPO, vous pouvez vous référer aux lignes directices du CEPD[22].

[20] **Fiche RGPD de la CNCC n° 5 :** *« Action #2 : Obtenez des garanties de la part de vos sous-traitants et partenaires. Vous devez formaliser dans vos contrats avec ces prestataires que toutes les règles requises sont mises en œuvre par leurs soins pour que les données que vous traitez et qu'ils sont susceptibles d'héberger sont protégées dans le respect du RGPD ».*

[21] **Fiche RGPD de la CNCC n° 3 :** *« Action #1 Désignez un référent pour structurer votre démarche : Identifiez une personne au sein de vos équipes pour piloter l'ensemble des actions à mettre en œuvre pour assurer la conformité de votre cabinet. Dans cette fonction de mise en œuvre de la conformité cette personne pourra entre autres organiser la documentation de votre conformité ».*

[22] Lignes directrices du CEPD concernant les délégués à la protection des données, en date du 13 décembre 2016 et du 5 avril 2017.

3. Focus sur l'obligation d'établir un registre des traitements

3.1 Objet et contenu du registre des traitements (article 30 du RGPD)

Aux termes de l'article 30 du RGPD, chaque responsable du traitement doit tenir un registre des traitements effectués sous sa responsabilité, devant contenir *a minima* :

- *« Le **nom et les coordonnées du responsable du traitement** et le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données.*
- *Les **finalités** du traitement.*
- *Une description des **catégories de personnes concernées** et des **catégories de données à caractère personnel.***
- *Les **catégories de destinataires** auxquelles les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales.*
- *Le cas échéant, **les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale**, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées.*
- *Dans la mesure du possible, **les délais prévus pour l'effacement** des différentes catégories de données.*
- *Dans la mesure du possible, une **description générale des mesures de sécurité techniques et organisationnelles** visées à l'article 32 paragraphe 1 ».*

> *À noter :* Cette liste ne constitue qu'un minimum. Il est recommandé de détailler davantage votre registre des traitements. Comme dans le modèle annexé à la présente fiche, vous pouvez ajouter des rubriques à votre registre (modalités d'information des personnes concernées, les sous-finalités du traitement, etc.).

3.2 La tenue du registre des traitements en pratique

Mon cabinet est-il obligé de tenir un registre des traitements ?

Oui, peu importe le nombre de salariés au sein de votre cabinet, vous êtes nécessairement amené en tant que commissaire aux comptes à traiter de manière régulière des données personnelles, ce qui vous oblige à tenir un registre des activités de traitement.

> Tout cabinet de commissariat aux comptes (quel que soit le nombre de salariés), doit établir et maintenir à jour un registre des traitements qu'il opère.

Quelle forme doit prendre un registre des traitements ? Où trouver des modèles ?

Les textes légaux et règlementaires n'imposent aucune forme ni aucun support particulier au registre. Il peut s'agir d'un tableau Excel, Word, ou même d'un logiciel administré par une personne en charge de la protection des données au sein de la structure.

Pour aider les professionnels dans leur conformité, la CNIL a publié un modèle simplifié de registre des traitements ainsi que son propre registre des traitements.

Un modèle de registre des traitements validé par la CNCC figure également en annexe de cette fiche. Ce modèle de registre des traitements n'est pas exhaustif mais vise à vous fournir des exemples des principaux traitements mis en œuvre par les commissaires aux comptes dans le cadre de leurs missions. (Cf. annexe 1 modèle CNCC de registre des traitements)

Comment établir et tenir à jour son registre des traitements ?

Pour établir un registre des traitements, il convient d'effectuer au préalable une « cartographie » des traitements mis en œuvre au sein de votre cabinet/entreprise. Cette démarche consiste à identifier et recenser les différents traitements opérés par votre cabinet dans le cadre de son activité (Cf. Commandement n° 6 *« Le RGPD tu respecteras »*[23]).

Parmi les traitements les plus courants mis en œuvre par un cabinet de commissaires aux comptes figurent la gestion de la relation contractuelle avec les entités contrôlées, la gestion des salariés, les traitements propres aux missions du commissaire aux comptes (missions de certification, missions d'audit, SACC, archivage des dossiers…).

Pour chaque traitement, il convient donc de lister :

- Le nom du responsable de traitement.
- Les catégories de données traitées, et notamment les catégories dites « particulières »[24] par exemple que le Commissaire aux comptes a accès à des informations relatives à des condamnations pénales dans le cadre de ses diligences sur les provisions sur litige).
- Les finalités pour lesquelles ces données sont collectées.
- La durée pendant laquelle ces données sont conservées.
- Le lieu où elles sont hébergées et/ou transférées (pays tiers n'assurant pas un niveau de protection adéquat[25]).
- La liste des sous-traitants susceptibles d'intervenir dans le traitement de ces données.
- Les mesures de sécurité mises en place pour protéger les données.

À noter : Un registre n'est jamais définitif. Il est évolutif et doit être maintenu à jour au fur et à mesure de l'activité de votre cabinet (intégration des nouveaux traitements, des nouvelles mesures de sécurité mises en place…). Il est recommandé d'instaurer un processus documenté de revue périodique du registre.

***

[23] **Commandement n° 6 :** *« Étape 2 : Cartographiez vos traitements de données personnelles existant dans le cabinet. Faites un inventaire des traitements de données personnelles mis en œuvre pour évaluer les pratiques, identifier les risques et arrêter un plan d'action ».*

[24] L'article 6 de la Loi informatique et Libertés et l'article 9 du RGPD définissent les données dites sensibles, dont le traitement est en principe interdit. Il s'agit des données *« qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique […], des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la sanét ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».*

[25] https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Glossaire du Guide :

« Règlementation applicable » désigne notamment le Règlement Général sur la Protection des Données (UE) n° 2016/679 (**« RGPD »**) et/ou tous décrets d'application ou lois nationales équivalentes, dans leur version en vigueur, en particulier la loi « Informatique et libertés » n° 78-17 du 6 janvier 1978 (**« loi informatique et liberté »**).

Les termes **« délégué à la protection des données », « données à caractère personnel », « données sensibles », « traitement »** sont définis au lexique numérique de la CNCC.

Les termes **« responsable du traitement »**[26] et **« sous-traitant »**[27] ont la définition qui leur est donnée dans le RGPD.

[26] **Article 4.7 du RGPD :** *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».*

[27] **Article 4.8 du RGPD :** *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».*

Annexe 1 – Fiches de traitements propres au commissaire aux comptes

1. Traitement de données à caractère personnel propre aux missions légales ou contractuelles du commissaire aux comptes		
N°/REF		
Date de création du traitement		
Dernière mise à jour		
Application(s)/logiciels concernée(s)	Nom de l'application/du logiciel : Nom de l'éditeur :	Commentaires :
Acteurs du traitement		
Responsable du traitement de données à caractère personnel*	Nom :	Coordonnées *(adresse postale, email, tél)* :
Délégué à la protection des données*	Nom : Société du DPO (si DPO externe) :	Cordonnées *(adresse postale, email, tél)* :
Représentant légal du responsable du traitement	Nom :	Cordonnées *(adresse postale, email, tél)* :
Responsable(s) conjoint(s)	Nom :	Coordonnées *(adresse postale, email, tél)* :
Sous-traitant *(à décliner en autant de sous-traitants)*	Nom :	Coordonnées *(adresse postale, email, tél)* :
Destinataire(s)*	1. Personnes externes contribuant à l'exécution de la mission (actuaires, experts internes et externes, réviseurs indépendants en charge du contrôle interne, collaborateurs externes). 2. Personnes en charge du contrôle qualité interne (à préciser au sein de chaque cabinet) et externe (régulateurs français tels que le H3C et l'AMF et régulateurs étrangers selon les accords bilatéraux conclus avec la France). 3. Autorités judiciaires et administratives (greffe des tribunaux de commerce, auxiliaires de justice, etc.). 4. Gouvernement d'entreprise (conseils d'administration, surveillance et autres organes de l'entité contrôlée). 5. Sous-traitants au sens du RGPD (prestataires IT, hébergeurs, etc.).	Type de destinataires : ***Internes et externes***

1. Traitement de données à caractère personnel propre aux missions légales ou contractuelles du commissaire aux comptes		
Finalités du traitement*		
Finalité 1	Mission de contrôle légal	
Sous-finalité 1	Certification des comptes	
Sous-finalité 2	Services autres que la certification des comptes (SACC) légaux (tels que l'établissement du rapport spécial, attestation des rémunérations, augmentation du capital…)[28].	
Sous-finalité 3	Procédures d'alerte	
Finalité 3	Missions légales ponctuelles (telles que le commissariat à la transformation, à la fusion, aux apports et aux avantages particuliers…)	
Finalité 1	Obligation légale à laquelle le responsable du traitement est soumis	
Finalité 3	Obligation légale à laquelle le responsable du traitement est soumis	
Catégories de personnes concernées*		
1. Personnel de l'entité contrôlée (dirigeants, salariés, stagiaires…). 2. Personnel du cabinet du commissaire aux comptes et, le cas échéant, collaborateurs et réviseurs indépendants externes. 3. Actionnaires et mandataires de l'entité contrôlée. 4. Experts (actuaires, avocats…). 5. Toute partie prenante de l'entité contrôlée (prestataires, clients de l'entité contrôlée, fournisseurs…).		
Catégories de données traitées et durées de conservation		
Données d'identité	Nom, prénoms, date et lieu de naissance, genre, nationalité, langue natale…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données de contact	Personnelles et/ou professionnelles : email, adresse postale, téléphone, fax, Messenger…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).

[28] Cf. Guide d'application de la CNCC de novembre 2018 sur les SACC à l'attention des entreprises, des comités d'audit, des conseils d'administration et de surveillance et des commissaires aux comptes : https://doc.cncc.fr/docs/services-autres-que-la-certifica/attachments/guide-sacc

1. Traitement de données à caractère personnel propre aux missions légales ou contractuelles du commissaire aux comptes		
Données de situation familiale	Situation maritale, nombre d'enfants, lien de parenté, régime matrimonial…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données professionnelles	Employeur, adresse de l'employeur, poste, grade, date d'entrée et de sortie, blâme, évaluation, formation, expérience, diplômes et certifications, licenciement et motif, CSP…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données patrimoniales et financières	Salaires et revenus, loyer, rente, personne(s) à charge, patrimoine immobilier, patrimoine financier (assurance vie, PEA…), taux d'imposition…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données de santé	Handicap, NIR, dates de congés maladie…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données bancaires	RIB, IBAN, interdit bancaire, banque et numéros de carte bleue, solde du compte…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données judiciaires	Infractions et condamnations (motifs, date, sanctions…)	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans(art. 9-1 du Code de procédure pénale).

1. Traitement de données à caractère personnel propre aux missions légales ou contractuelles du commissaire aux comptes		
Données comptables	N°, date, montant, émetteur dans les objets de type factures, décaissements, encaissements, recouvrement…	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Données administratives	Informations contenues sur les CNI, passeport, titre de séjour, visa (n°, dates, délivré le, par, date d'expiration…)	***[Celle définie par le Cabinet en considération des périodes de prescription]***, au minimum 6 ans (art. R. 821-68 du Code de commerce) et au maximum 12 ans (art. 9-1 du Code de procédure pénale).
Transfert de données vers un pays tiers à l'UE ou vers une organisation internationale* [Oui / Non]		
Si oui, organisme destinataire	Nom de l'outil / du sous-traitant : Pays : Type de garanties :	Type de garantie mise en œuvre : *(Clauses contractuelles types, BCR en cas de transferts au sein d'un réseau de commissaire aux comptes …)*
Mesures de sécurité techniques / organisationnelles*	Mesures de sécurité techniques Mesures de sécurité organisationnelles Mesures de sécurité physiques *(faire référence aux politiques / guides de sécurité)*	
Information des personnes concernées	L'information des salariés, actionnaires, mandataires et parties prenantes de l'entité contrôlée par le commissaire aux comptes n'est pas obligatoire (cf. Art. 14, 5°d. du RGPD). Le commissaire aux comptes informe l'entité contrôlée des traitements réalisés dans sa lettre de mission et sa politique de confidentialité. Le personnel du cabinet du commissaire aux comptes est informé des traitements réalisés *via* ***[à adapter : la charte informatique, la politique de confidentialité, le contrat de travail…]***	
Exemples d'outils utilisés dans le cadre du traitement	Solutions technologiques nécessaires à l'accomplissement de la mission du commissaire aux comptes *(par exemple : outils de communication, de travail collaboratif avec l'entité contrôlée, solutions de partage de documents, outils d'extraction et d'analyse de données permettant de faciliter les vérifications et contrôles opérés à l'occasion des missions et services précités).*	

1. Traitement de données à caractère personnel propre aux missions légales ou contractuelles du commissaire aux comptes	
Analyse d'impact relative à la protection des données	
Nécessaire ?	**Non** L'article 35 du RGPD dispose que le responsable du traitement effectue une analyse d'impact lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. L'article 35 § 3 du RGPD énonce les trois principaux cas dans lesquels une analyse d'impact est nécessaire : 1. Évaluation systématique et approfondie d'aspect personnel fondé sur un traitement automatisé. 2. Traitement à grande échelle de catégories particulières de données. 3. Surveillance systématique à grande échelle d'une zone accessible au public. Le Comité Européen de la Protection des Données (CEPD) a complété cette liste dans ses lignes directrices relatives à l'analyse d'impact. En l'espèce, le traitement ne répond ni aux critères énoncés à l'article 35 du RGPD, ni à ceux énoncés par le CEPD. Par ailleurs, il convient de noter que le commissaire aux comptes est soumis au secret professionnel dans le cadre de ses missions et que le présent traitement a pour base juridique le respect d'une obligation légale incombant au commissaire aux comptes. **Une analyse d'impact n'apparaît donc pas nécessaire pour ce traitement.** (*Même si les critères de l'article 35 du RGPD et le CEPD ne sont pas remplis, vous pouvez néanmoins effectuer une analyse d'impact si vous l'estimez nécessaire*[29])

[29] Pour cela, vous pouvez utiliser le logiciel open source mis à votre disposition par la CNIL : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

2. Traitement de données à caractère personnel propre à la gestion et l'archivage des dossiers du commissaires aux comptes		
N°/REF		
Date de création du traitement		
Dernière mise à jour		
Acteurs		
Responsable du traitement de données à caractère personnel*	Nom :	Coordonnées *(adresse postale, email, tél)* :
Délégué à la protection des données*	Nom : Société du DPO (si DPO externe) :	Cordonnées *(adresse postale, email, tél)* :
Représentant	Nom :	Cordonnées *(adresse postale, email, tél) :*
Responsable(s) conjoint(s)	Nom :	Coordonnées *(adresse postale, email, tél)* :
Sous-traitant (à décliner en autant de sous-traitants)	Nom :	Coordonnées *(adresse postale, email, tél)* :
Destinataire(s)*	1. Personnel habilité du cabinet du commissaire aux comptes (gestion du contentieux et de la compliance au sein du cabinet) 2. Autorités judiciaires et administratives (greffe du tribunal de commerce, auxiliaires de justice, etc.) 3. Sous-traitants au sens du RGPD (prestataires IT, hébergeurs, etc.).	Type de destinataire : **Internes et externes**
Finalité du traitement*		
Finalité 1	Conservation des dossiers du commissaire aux comptes en vue d'assurer la défense du commissaire aux comptes en cas de litige avec l'entité contrôlée ou un tiers.	
Finalité 2	Accomplissement de l'obligation légale d'archivage incombant au commissaire aux comptes (art. R. 821-68 du Code de commerce).	
Base légale associée au traitement*		
Finalité 1	Intérêt légitime du commissaire aux comptes.	
Finalité 2	Obligation légale à laquelle le responsable du traitement est soumis.	

2. Traitement de données à caractère personnel propre à la gestion et l'archivage des dossiers du commissaires aux comptes		
Catégories de personnes concernées*		
1. Personnel de l'entité contrôlée (dirigeants, salariés, stagiaires…). 2. Personnel du cabinet du commissaire aux comptes. 3. Actionnaires et mandataires de l'entité contrôlée. 4. Experts du commissaire aux comptes (actuaires, avocats etc.). 5. Toute partie prenante de l'entité contrôlée (prestataires, clients de l'entité contrôlée, etc.).		
Catégories de données traitées et durées de conservation*		
Données d'identité	Nom, prénoms, date et lieu de naissance, genre, nationalité, langue natale…	10 à 12 ans selon les règles de prescription civiles et pénales.
Données de contact	Personnelles et/ou professionnelles : email, adresse postale, téléphone, fax, Messenger…	10 à 12 ans selon les règles de prescription civiles et pénales.
Données de situation familiale	Situation maritale, nombre d'enfants, lien de parenté, régime matrimonial…	10 à 12 ans selon les règles de prescription civiles et pénales.
Données professionnelles	Employeur, adresse de l'employeur, poste, grade, date d'entrée et de sortie, blâme, évaluation, formation, expérience, diplômes et certifications, licenciement et motif, CSP…	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code de procédure pénale).
Données patrimoniales et financières	Salaires et revenus, loyer, rente, personne(s) à charge, patrimoine immobilier, patrimoine financier (assurance vie, PEA…), taux d'imposition…	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code de procédure pénale).
Données de santé	Handicap, NIR, dates de congés maladie…	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code de procédure pénale).
Données bancaires	RIB, IBAN, interdit bancaire, banque et numéros de carte bleue, solde du compte…	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code de procédure pénale).
Données judiciaires	Infractions et condamnations (motif, date, sanctions…).	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code pénal).

2. Traitement de données à caractère personnel propre à la gestion et l'archivage des dossiers du commissaires aux comptes		
Données comptables	N°, date, montant, émetteur dans les objets de type factures, décaissements, encaissements, recouvrement…	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code de procédure pénale).
Données administratives	Informations contenues sur les CNI, passeport, titre de séjour, visa (n°, dates, délivré le et par, date d'expiration…).	10 à 12 ans selon les règles de prescription civiles et pénales (art. 9-1 du Code de procédure pénale).
Transfert de données vers un pays tiers à l'UE ou vers une organisation internationale* [Oui / Non]		
Si oui, organisme destinataire	Nom de l'outil / du sous-traitant : Pays : Type de garanties :	Type de garantie mise en œuvre : *(Clauses contractuelles types, BCR en cas de transferts au sein d'un réseau de commissaire aux comptes …)*
Mesures de sécurité techniques / organisationnelles*	Mesures de sécurité techniques Mesures de sécurité organisationnelles Mesures de sécurité physiques *(faire référence aux politiques/guides de sécurité)*	
Information des personnes concernées	L'information des actionnaires, mandataires, prestataires et parties prenantes de l'entité contrôlée n'est pas obligatoire. Le commissaire aux comptes informe l'entité contrôlée des traitements réalisés dans sa lettre de mission du commissaire aux comptes et dans sa politique de confidentialité. Le personnel du cabinet du commissaire aux comptes est informé *via* ***[à adapter : la charte informatique, la politique de confidentialité, le contrat de travail…]***	

2. Traitement de données à caractère personnel propre à la gestion et l'archivage des dossiers du commissaires aux comptes		
Analyse d'impact relative à la protection des données		
Nécessaire ?	**Non** L'article 35 du RGPD dispose que le responsable du traitement effectue une analyse d'impact lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. L'article 35 § 3 du RGPD énonce les trois principaux cas dans lesquels une analyse d'impact est nécessaire : 1. Évaluation systématique et approfondie d'aspect personnel fondé sur un traitement automatisé. 2. Traitement à grande échelle de catégories particulières de données. 3. Surveillance systématique à grande échelle d'une zone accessible au public.	Décision : [Oui / Non] N/A
	Le Comité Européen de la Protection des Données (CEPD) a complété cette liste dans ses lignes directrices relatives à l'analyse d'impact. En l'espèce, le traitement ne répond ni aux critères énoncés à l'article 35 du RGPD, ni à ceux énoncés par le CEPD. Par ailleurs, il convient de noter que le commissaire aux comptes est soumis au secret professionnel dans le cadre de ses missions. **Une analyse d'impact n'apparaît donc pas nécessaire pour ce traitement.** *(Même si les critères de l'article 35 du RGPD et le CEPD ne sont pas remplis, vous pouvez néanmoins effectuer une analyse d'impact si vous l'estimez nécessaire[30].)*	

[30] Pour cela, vous pouvez utiliser le logiciel open source mis à votre disposition par la CNIL : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Statut du commissaire aux comptes

Fiche n° 2

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

⇨ Le commissaire aux comptes doit être qualifié de « responsable du traitement » pour les raisons suivantes :

1. Il **conserve la maîtrise des finalités et des moyens** des traitements opérés : la mission de certification des comptes annuels **est fixée par la loi**[31].
2. Il dispose **d'une indépendance** dans l'exercice de ses missions et l'établissement de ses rapports et attestations effectués sous **son propre nom et sa responsabilité.**
3. Il **détermine seul les moyens techniques et organisationnels** à mettre en place (par exemple : choix des outils et technologies utilisés lors de sa mission, mesures et procédures de sécurité internes, etc.).

⇨ Le commissaire aux comptes demeure responsable du traitement pour l'ensemble des missions qu'il peut être amené à opérer, y compris dans le cadre des SACC, compte tenu de la forte autonomie et de l'expertise qu'il conserve dans l'accomplissement de ces services **(2.2).**

⇨ Le commissaire aux comptes devra informer ses clients de son statut **(3.1)** et s'assurer d'encadrer contractuellement ses rapports avec les experts auxquels il peut faire appel qui agissent également en tant que responsables de traitement **(3.2).**

[31] Code de déontologie – Article liminaire du Titre II : *« Le commissaire aux comptes exerce une mission d'intérêt général dans les conditions fixées par la loi ».*

Statut du commissaire aux comptes

Sommaire

Contexte

Les commissaires aux comptes sont amenés, dans le cadre de leur activité professionnelle, à réaliser un certain nombre de traitements de données personnelles en collectant, consultant et analysant des documents, pièces ou fichiers dématérialisés ou en format papier (tels que des documents comptables, factures, fiches de paie, etc.) qui contiennent des données à caractère personnel essentiellement des fournisseurs, clients et employés de leurs clients.

Par ailleurs, ces documents sont couverts par le secret professionnel. Ces données à caractère personnel traitées par le commissaire aux comptes à l'occasion des missions confiées sont collectées indirectement par celui-ci, par l'intermédiaire de son client ou de tiers mandatés par ce dernier, tels que leurs avocats.

S'agissant des traitements réalisés par le commissaire aux comptes dans le cadre de ses missions confiées par ses clients, le commissaire aux comptes intervient en tant que responsable du traitement, au regard des traitements qu'il réalise. La Réglementation applicable en matière de protection des données opère en effet une distinction entre les obligations qui incombent au « responsable du traitement » et celles qui incombent au « sous-traitant » (Cf. Chapitre IV « Responsable du traitement et sous-traitant » du RGPD).

Certains clients considèrent, à tort, leur commissaire aux comptes comme l'un de leurs « sous-traitants », au sens de la Réglementation applicable en matière de protection des données, et lui demandent de signer un « contrat de sous-traitance » aux termes duquel le commissaire aux comptes doit s'engager à se conformer aux instructions de son client, ainsi qu'à un certain nombre d'obligations notamment en matière de sécurité, choix des fournisseurs de technologies ou sous-traitants.

La signature de tels engagements n'est pas compatible avec l'indépendance, l'expertise et l'autonomie du commissaire aux comptes.

L'objectif de cette fiche est d'expliciter :

a. Les critères retenus par la CNIL permettant de distinguer le statut de responsable du traitement de celui de sous-traitant.

b. Les bases juridiques permettant de justifier le statut de responsable du traitement du commissaire aux comptes.

c. Les principales implications induites pour le commissaire aux comptes, notamment en matière d'information des entités contrôlées et personnes concernées, ou lorsqu'il s'adjoint les services de tiers (autres experts).

1. Les critères de différenciation entre les statuts de « responsable du traitement » et celui de « sous-traitant »

Le **responsable du traitement** détermine les moyens et les finalités du traitement de données personnelles. En d'autres termes, le responsable du traitement est celui qui détermine quelles données personnelles sont traitées, ainsi que pourquoi et comment elles sont ou doivent être traitées.

Le **sous-traitant**, quant à lui, ne traite les données personnelles que pour le compte et sur instructions du responsable du traitement. Il est un « exécutant » et doit généralement solliciter l'accord quasi systématique du responsable du traitement pour tout changement (changement du niveau de sécurité, changement d'un sous-traitant ultérieur par exemple).

La CNIL a fourni, dans un « Guide du sous-traitant »[32], une série de critères d'appréciation qui permettent de distinguer le responsable du traitement du sous-traitant :

1. Le **niveau d'instructions donné par le client au prestataire :** ce critère permet de définir le degré d'autonomie qui est laissé à une entité dans la réalisation de sa mission de services.
2. Le **degré de contrôle** exercé par le client sur son prestataire : ce critère permet de définir le degré de liberté laissé au prestataire pour l'accomplissement de sa prestation.
3. **La valeur ajoutée / l'expertise du prestataire :** plus le prestataire est expert dans son domaine et décide des moyens à mettre en place dans le cadre de la réalisation des prestations, plus il sera considéré comme responsable du traitement. Si le prestataire n'a finalement qu'un rôle d'exécutant ou de fournisseur de moyens (simple mise à disposition d'une data room électronique par exemple), sans valeur ajoutée, il sera plutôt considéré comme un sous-traitant.
4. Le degré de **transparence sur le recours à un prestataire :** ce critère permet de définir si le prestataire agit en son nom propre ou s'il agit, dans le cadre des prestations dont il a la charge, au nom de son client.

En outre, il conviendrait de rajouter à ces critères :

5. La définition des **moyens techniques :** le fait que le prestataire utilise ses propres ressources techniques ou celles qui seraient définies par le client, voire l'infrastructure technique de ce dernier constitue également un indice permettant d'établir qui définit les moyens techniques du traitement.

[32] CNIL – Guide du sous-traitant – Edition septembre 2017.

2. Le statut de responsable du traitement du commissaire aux comptes

2.1 L'application des critères susvisés conduit à qualifier le commissaire aux comptes de « responsable » des traitements qu'il opère dans le cadre de sa mission :

La mission de certification des comptes annuels de l'entité contrôlée est une mission d'**intérêt général**, ce qui justifie que le commissaire aux comptes conserve la maîtrise des finalités et des moyens des traitements qu'il réalise, à savoir l'approche d'audit et les diligences qu'il détermine en fonction de sa stratégie d'audit qu'il mettra en œuvre dans le cadre de cette mission.

L'entité contrôlée ne définit pas la mission du commissaire aux comptes, de même que le contenu du rapport qu'il présente. Cette mission est définie au Code de commerce, dont l'article L. 823-9 précise que :

« Les commissaires aux comptes certifient, en justifiant de leurs appréciations, que les comptes annuels sont réguliers et sincères et donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de la situation financière et du patrimoine de la personne ou de l'entité à la fin de cet exercice. »

Le commissaire aux comptes est nécessairement **indépendant dans l'exercice de ses missions** et dans l'établissement de ses rapports ou attestations, qui sont établis **sous son propre nom** (et non celui de l'entité contrôlée) et sa responsabilité. Il ne peut donc recevoir aucune « instruction » de l'entité contrôlée dans l'exercice de sa mission.

Cette indépendance est renforcée par les dispositions du Code de commerce et plus particulièrement par l'article L. 823-13 selon lequel le commissaire aux comptes :

- dispose de la possibilité de se faire assister dans l'exercice de ses missions :

  *« Pour l'accomplissement de leurs contrôles, les commissaires aux comptes peuvent, **sous leur responsabilité,** se faire assister ou représenter par tels experts ou collaborateurs **de leur choix,** qu'ils font connaître nommément à la personne ou à l'entité dont ils sont chargés de certifier les comptes. » ;*

- a la capacité de consulter tous documents (qu'ils contiennent ou non des données à caractère personnel) :

  *« À toute époque de l'année, les commissaires aux comptes, ensemble ou séparément, opèrent **toutes vérifications et tous contrôles qu'ils jugent opportuns** et peuvent se faire communiquer sur place **toutes les pièces qu'ils estiment utiles** à l'exercice de leur mission et notamment tous contrats, livres, documents comptables et registres des procès-verbaux. ».*

Le commissaire aux comptes est donc libre dans l'exercice de sa mission et expressément désigné comme un tiers habilité à être destinataire de divers documents qui, intrinsèquement, sont susceptibles de comporter des données à caractère personnel, s'il le juge utile pour l'accomplissement de sa mission.

S'agissant de la définition de la **durée de conservation des données** pour les dossiers et documents établis par le commissaire aux comptes dans le cadre de l'exercice du contrôle légal et autres missions et prestations qu'il exerce, le commissaire aux comptes est soumis à une obligation de conservation de ses dossiers et documents (y inclus ceux contenant des données à caractère personnel) pendant une durée de 6 ans, *« même après la cessation des fonctions »* *(Cf. Article R. 821-68 du Code de commerce)* ou une durée plus longue tenant compte des règles de prescriptions légales applicables. C'est donc le commissaire aux comptes[33] qui détermine les durées de conservation et non l'entité contrôlée qui n'a pas de légitimité à imposer une durée de conservation des données qui lui serait propre.

Le commissaire aux comptes **détermine également seul les moyens techniques et organisationnels à mettre en place** lors des traitements effectués, notamment le choix des outils et technologies utilisés lors de sa mission, les mesures et procédures de sécurité internes qui sont nécessaires à la préservation de la confidentialité des données couvertes par le secret professionnel, la définition de ses équipes qui vont traiter les données…

« Les commissaires aux comptes, ainsi que leurs collaborateurs et experts, sont astreints au secret professionnel pour les faits, actes et renseignements dont ils ont pu avoir connaissance à raison de leurs fonctions » *(Cf. Article L. 822-15 du Code de commerce).*

Le positionnement de responsable de traitement a été confirmé par les lignes directrices du CEPD adoptées en septembre 2020[34].

2.2 Y aurait-il des exceptions à cette qualification de « responsable du traitement » ?

Certaines entités contrôlées considèrent être **« responsables conjoints »** des traitements réalisés par un commissaire aux comptes.

Cette appréciation ne peut être retenue car les finalités des traitements de données personnelles réalisés par l'entité contrôlée d'une part et le commissaire aux comptes d'autre part, **sont distinctes** :

- l'entité contrôlée réalise des traitements ayant pour finalité notamment l'établissement de ses comptes ; tandis que
- le commissaire aux comptes réalise des traitements propres à sa mission pour donner son opinion sur ceux-ci et les certifier, ou dans le cadre de ses autres missions légales.

Lorsqu'un commissaire aux comptes exerce d'**autres missions que celle de certification des comptes** (SACC par exemple), relevant des différentes catégories de services pouvant être rendus par un commissaire aux comptes selon le H3C[35] (telles qu'indiquées dans l'annexe 1 de la fiche n° 1 du guide : « *Registre* »), le commissaire aux comptes demeure responsable des

[33] À titre informatif, le Comité Européen de la Protection des Données (CEPD, anciennement le G29) considère également que l'entité qui définit des aspects essentiels du traitement, et notamment la durée de conservation des données, doit être considérée comme responsable du traitement.

[34] Voir page 14
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

[35] H3C, FAQ sur l'application des nouvelles dispositions encadrant le contrôle légal des comptes (version du 19 juillet 2018).

traitements qu'il opère, dans la mesure où, là encore, il détermine seul les finalités et les moyens de traitement.

Ceci vaut également dans le cadre des **« procédures convenues »**.

Les procédures convenues sont des procédures de contrôle spécifiques, en dehors de toute obligation légale, demandées au commissaire aux comptes à l'initiative d'une entité.

Le Communiqué de la CNCC intitulé « Référence aux normes ou à la doctrine pour les SACC fournis à la demande de l'entité (qui remplace la NEP n° 9040 de 2008) indique que ces procédures sont effectuées conformément aux dispositions applicables du Code de commerce et du Code de déontologie (cf. article L. 820-1-1 du Code de commerce tel que créé par la loi Pacte).

Par conséquent, l'ensemble des principes déontologiques qui régissent la profession, au rang desquels figure le **principe d'indépendance**, demeurent pleinement applicables.

Par ailleurs, l'article 1er du Code de déontologie dispose que *« le présent code définit la déontologie à laquelle le commissaire aux comptes est soumis quelle que soit la nature des missions ou des prestations qu'il fournit »*. Par conséquent, le commissaire aux comptes conserve son indépendance et son autonomie tant dans le cadre de ses missions légales que de ses missions contractuelles.

- *« Le commissaire aux comptes convient avec l'entité contrôlée des informations, données, documents ou éléments du contrôle interne sur lesquels portent les procédures à mettre en œuvre, de la nature de l'étendue et du calendrier des procédures à mettre en œuvre, des modalités de restitution des travaux et des constats qui en résultent, des conditions restrictives de diffusion du rapport »*. Ces rapports évoquent plutôt ceux entre deux **responsables du traitement, et non ceux d'un responsable du traitement vis-à-vis de son sous-traitant.**
- Dans tous les cas, le commissaire aux comptes peut refuser l'intervention au titre de SACC, d'une procédure convenue, démontrant là encore son niveau d'autonomie dans le choix et le déroulé de sa mission. Le commissaire aux comptes précise dans son rapport la portée et les limites de son intervention.
- Le rapport de procédures convenues doit faire référence à l**a doctrine professionnelle** en indiquant : *« Nos travaux sont effectués selon la doctrine professionnelle de la CNCC relative à cette intervention »*[36].

Enfin, dans le cadre d'une mission de **co-commissariat**, chaque commissaire aux comptes est responsable des traitements qu'il opère et détermine de manière indépendante les moyens nécessaires à sa mission dans le respect des normes professionnelles : il n'y a pas de responsabilité conjointe, au sens du RGPD, entre les co-commissaires aux comptes (Cf. Fiche n° 6 du guide « *Le RGPD dans un contexte co-CAC* »).

[36] Communiqué de la CNCC intitulé *« Référence aux normes ou à la doctrine pour les SACC fournis par le commissaire aux comptes à la demande de l'entité »*, paragraphe 2. « Attestation, procédures convenues, vérification des informations RSE par l'OTI ».

3. Conséquences induites de la qualification de Responsable du traitement

Le commissaire aux comptes, en qualité de responsable du traitement, dispose d'une autonomie certaine dans la réalisation des traitements qu'il opère dans le cadre de l'accomplissement de ses missions ou encore dans le cadre de la mise en œuvre des normes professionnelles et déontologiques qui lui sont applicables (Cf. Annexe jointe à la Fiche n° 1 du guide « *Gouvernance et Accountability* »). Il n'en demeure pas moins soumis aux obligations qui lui incombent au titre de la Règlementation applicable en matière de protection des données à caractère personnel.

En particulier, il lui incombe d'informer les entités contrôlées de son statut et de sécuriser les relations contractuelles avec les prestataires sous-traitants (au sens du RGPD) qu'il s'adjoint.

3.1 L'information des entités contrôlées et des personnes concernées

3.1.1 Informer l'entité contrôlée sur son statut de responsable du traitement

Le commissaire aux comptes devra formaliser son statut dans ses lettres de mission et conditions générales d'intervention.

Un modèle de lettre de réponse à une entité contrôlée qui souhaiterait faire signer un accord de sous-traitance à son commissaire aux comptes est joint en annexe 1 de la présente fiche. Ce modèle propose une motivation du statut de responsable du traitement du commissaire aux comptes.

3.1.2 Faut-il informer les personnes concernées dont les données sont collectées indirectement par l'intermédiaire de l'entité contrôlée ?

Les données à caractère personnel traitées par le commissaire aux comptes à l'occasion de sa mission sont collectées non pas directement auprès des personnes concernées, mais **indirectement**, par l'intermédiaire de l'entité contrôlée ou d'un tiers mandaté par cette dernière, qui lui remet des pièces et documents contenant des données à caractère personnel, essentiellement de ses salariés, fournisseurs ou clients (factures, bulletins de paie, déclarations sociales, etc.).

Lors de la collecte de données par l'entité contrôlée, il incombe à l'entité contrôlée, agissant en tant que responsable du traitement, d'informer les personnes concernées que le commissaire aux comptes est l'un des destinataires de leurs données personnelles.

Le commissaire aux comptes collecte les données utiles à sa mission par l'intermédiaire de l'entité contrôlée, donc **indirectement**. L'article 14.5 du RGPD prévoit dans ce cas plusieurs dérogations à l'obligation qui incombe au responsable du traitement de fournir des informations aux personnes concernées sur les traitements qu'il opère, et en particulier lorsque :

- *« la personne concernée dispose déjà de ces informations »* (Article 14 § 5 a) du RGPD) ; et
- *« (…) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membres, y compris une obligation légale de secret professionnel » (Article 14 § 5 d) du RGPD).*

Dès lors, en cas de collecte indirecte, le commissaire aux comptes sera dispensé, dans la majorité des cas, de fournir les informations obligatoires au titre du RGPD aux personnes concernées, dès lors que (i) les informations auront déjà été fournies par l'entité contrôlée, et/ou (ii) les informations sont soumises au secret professionnel incombant aux commissaires aux comptes.

En conséquence, dans vos rapports contractuels avec les entités contrôlées vous devrez :

- Rappeler aux entités contrôlées qu'elles doivent informer les personnes concernées de ce que leurs données peuvent être transférées aux commissaires aux comptes, et que
- Vous ne procéderez à aucune information additionnelle des personnes concernées conformément aux dispositions des articles 14 § 5 a) et d) du RGPD.

Pour plus d'informations sur les principes applicables et les recommandations en matière d'information des personnes concernées, veuillez-vous référer à la Fiche n° 4 du guide « *Transparence – Information* » (Cf. également Fiche RGPD de la CNCC n° 6 « *Adaptez vos traitements de données. Documentez votre démarche* »).

3.2 À l'égard des experts et collaborateurs externes qui assistent le commissaire aux comptes dans l'accomplissement de sa mission

Conformément à l'article L. 823-13 du Code de commerce :

« Pour l'accomplissement de leurs contrôles, les commissaires aux comptes peuvent, ***sous leur responsabilité****, se faire assister ou représenter par tels experts ou collaborateurs* ***de leur choix****, qu'ils font connaître nommément à la personne ou à l'entité dont ils sont chargés de certifier les comptes. »*

Compte tenu de la nature des missions et leur degré d'autonomie (conformément aux critères susvisés), ces experts et collaborateurs externes agissent en tant que responsables du traitement.

En conséquence, les transferts de données personnelles opérés entre le commissaire aux comptes et ces experts et collaborateurs externes seront des transferts de responsable du traitement à responsable du traitement (RT à RT).

Dès lors, il appartient au commissaire aux comptes de s'assurer :

- que l'expert/collaborateur externe adopte bien la qualification de responsable du traitement dans ses rapports contractuels avec le commissaire aux comptes ;
- que chacun s'engage contractuellement à se conformer à ses obligations au regard de la Règlementation applicable, en particulier s'agissant de la sécurité des données qui lui sont confiées ;
- d'encadrer contractuellement les transferts des données conformément à la Règlementation applicable, dès lors que l'expert/collaborateur externe est situé dans un pays tiers n'assurant pas un niveau de protection adéquat[37]. Le commissaire aux comptes doit utiliser le modèle de clauses contractuelles type « responsable du traitement à responsable du traitement » proposé par la commission européenne (Pour plus d'informations sur l'encadrement des transferts de données personnelles, vous pouvez vous référer à la Fiche n° 7 du guide « Transferts internationaux »).

[37] https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Annexe 1 – Projet pour avis CNCC

[CLIENT]
Fonction
Société
Adresse
Code Postal Localité
Pays

[Ville], le

Objet *: Statut de notre Cabinet au regard de la réglementation applicable en matière de protection des données personnelles*

Madame, Monsieur,

Nous faisons suite à *[nos derniers échanges du / votre lettre / courriel en date du]].*

Nous souhaitons vous apporter quelques précisions relatives aux traitements de données personnelles que nous sommes susceptibles d'effectuer dans le cadre de la mission de commissariat aux comptes que vous ***[souhaitez nous confier / nous avez confiée]*** (*la « Mission »*)), et notre statut au regard de la réglementation applicable en matière de protection des données à caractère personnel.

[Cette règlementation comprend notamment le Règlement Général sur la Protection des Données (UE) n° 2016/679 et/ou tous décrets d'application ou lois nationales équivalentes, dans leur version en vigueur, en particulier la loi « Informatique et libertés » n° 78 17 du 6 janvier 1978].

Dans le cadre de notre Mission de commissariat aux comptes, nous sommes susceptibles d'être destinataires de données à caractère personnel qui figurent dans les documents et pièces (notamment comptables) que nous sommes appelés à auditer. Nos travaux sont conduits selon les normes d'exercice professionnel et la doctrine professionnelle de la Compagnie Nationale des Commissaires aux Comptes (CNCC).

Le Commissaire aux Comptes détermine seul la finalité, les moyens essentiels et non essentiels des traitements opérés dans le cadre de sa Mission, et demeure en toutes circonstances un expert indépendant à l'égard de son client. Nous déterminons ainsi les moyens humains et techniques qui nous apparaissent appropriés pour mener à bien cette Mission.

Ce faisant, notre cabinet est responsable des traitements de données à caractère personnel qu'il opère dans l'exercice de ses missions au sens de la réglementation applicable en matière de protection des données personnelles. Dans ces conditions, notre Cabinet n'a pas à signer le document joint à votre ***lettre/courriel du [...]*** qui vise à encadrer les traitements de données personnelles réalisés par vos « sous traitants ».

Notre Cabinet est soumis aux obligations prévues par la réglementation applicable et qui lui incombent en sa qualité de « responsable de traitement ». Les traitements opérés restent circonscrits au périmètre de notre Mission et de nos attributions, pour des finalités déterminées, explicites et légitimes. Nous rappelons également que nous sommes tenus au secret professionnel, conformément à l'article Article L. 822 15 du Code de commerce.

Pour toute question complémentaire, veuillez consulter ***[notre politique de confidentialité]*** et/ou contacter notre ***[DPO/Délégué à la protection des données, point de contact sur ces sujets]*** aux coordonnées suivantes ***[...].***

[Formule de politesse]

[Signataire]

Gestion de la relation professionnelle

Fiche n° 3

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

L'objectif de cette fiche est de vous guider quant aux bonnes pratiques à mettre en œuvre tout au long du cycle de vie de votre relation professionnelle avec vos clients et prospects afin d'être conforme à la Réglementation applicable.

De l'entrée en contact avec un prospect jusqu'à la fin de la relation d'affaires, la gestion des données personnelles des clients et prospects doit respecter les grands principes de la Réglementation applicable (Fiche n° 1 du guide *« Gouvernance et accountability »*).

La constitution de votre base de prospects peut se faire de différentes façons (événements, réseaux sociaux professionnels, sollicitation, collecte via le site internet…) (1). Quel que soit le procédé utilisé, il convient de veiller principalement à :

- **Fournir aux personnes concernées certaines** informations obligatoires dans vos emails de sollicitation professionnelle **(1.1)**.
- **Ne collecter que les données dont vous avez besoin** (principe de minimisation) notamment lorsque celles-ci proviennent de réseaux sociaux professionnels **(1.2)**.
- **Ne pas recourir aux services de sociétés tierces utilisant des procédés non-conformes** à la Réglementation applicable, comme le *« scraping »* par exemple **(1.3)**.
- **Vérifier la présence de mentions d'information** sur vos formulaires de collecte et d'un **bandeau cookies** conforme aux exigences de la CNIL sur votre site internet **(1.4)**.

Lorsque le prospect devient un client, l'obligation de connaître son client (dite « KYC » *Know Your Client*) s'applique. Ce traitement requiert la mise en place de mesures de sécurité renforcées en cas de conservation des documents collectés et doit figurer dans votre registre des activités de traitements **(2)**. Un modèle de fiche de traitement KYC du commissaire aux comptes est joint en annexe 1 de cette fiche.

Dans la gestion courante des données de vos clients et prospects, il est recommandé d'opter pour un outil CRM *« Privacy by Design »* et de vérifier régulièrement les zones de commentaires libres **(3)**.

Enfin, une attention particulière doit être portée aux durées de conservation. De manière générale, il convient de retenir que les données personnelles de vos clients et prospects ne peuvent pas être conservées indéfiniment et ne doivent pas être supprimées trop tôt **(4)**. Un tableau de synthèse des durées de conservation figure en annexe 2 de cette fiche.

Gestion de la relation professionnelle

Sommaire

1. Étape 1 – Comment constituer et enrichir sa base de clients et prospects ?

Nous évoquerons ci-après les bonnes pratiques à mettre en œuvre selon le type de situations.

1.1 Collecte de données à l'occasion de salons, conférences ou autres événements professionnels

Lorsque vous participez à, ou organisez des événements professionnels, seuls ou en collaboration avec d'autres professionnels ou sponsors, vous pouvez être amenés à collecter et/ou échanger des données de clients et prospects.

Bien entendu, il est légitime de pouvoir enregistrer dans vos bases de données de contacts les coordonnées des personnes qui vous transmettent leur carte de visite, bien que cette pratique tende à disparaître au profit de mises en relation *via* des applications et/ou réseaux sociaux professionnels.

Si vous êtes l'organisateur de l'événement, il se peut que vous fassiez appel à des sociétés d'événementiel spécialisées. Il faudra alors être clair, à l'égard des participants invités, sur les rôles et responsabilités de chacun : en général, la société d'événementiel intervient plutôt en qualité de « sous-traitant » (au sens de la Réglementation applicable en matière de protection de données personnelles), tandis que le commissaire aux comptes est responsable du traitement (Cf. Fiche n° 2 du guide *« Statut du Commissaire aux comptes »*).

Comment cela se traduit-il en pratique ?

- ⇨ C'est vous qui devez informer les participants des traitements réalisés sur leurs données et des destinataires de leurs données, ainsi que de l'existence de sous-traitants (notamment).
- ⇨ Ce sont vos mentions d'information qui doivent être accessibles dans les mailings, sites web, prospectus, formulaires d'inscription et autres supports associés à l'événement en question, et non celles de la société d'événementiel (votre sous-traitant au sens RGPD).
- ⇨ C'est à vous de prendre les dispositions pour que l'organisateur (sous-traitant) (i) respecte vos instructions, (ii) prenne les mesures de sécurité nécessaires pour la préservation de l'intégrité des données, et (iii) s'abstienne de les utiliser à des fins propres (Cf. Fiche du guide n° 10 *« Gestion de la sous-traitance »*).
- ⇨ Lorsque la société d'événementiel « ouvre » son carnet d'adresses ou lorsque vous organisez un événement en partenariat avec une autre société pour convier ses contacts à un événement, vous serez responsable du traitement des données des personnes qui s'inscrivent à l'événement.

Attention : selon les organisateurs, la distinction n'est pas toujours évidente à opérer et vous devrez vous assurer que les outils qu'ils utilisent permettent de faire figurer vos mentions d'informations et votre politique de confidentialité.

En conclusion

• Les bonnes pratiques :

- ✓ Informer clairement les invités de l'identité du/des **responsable(s) du traitement**[38] (vous et, le cas échéant d'autres sociétés co-organisatrices de l'événement) de leurs données personnelles : cette information doit figurer dans les mailings, sur la page de l'événement, les brochures et bulletins d'inscription, etc., au même titre que les autres éléments d'informations prévus par la Réglementation applicable (Cf. Fiches n° 1 *« Gouvernance et Accountability »* et n° 4 *« Transparence – Information »* du guide). Cette information pourra être détaillée par un renvoi vers une politique de confidentialité[39].
- ✓ Privilégier des sociétés d'événementiel / solutions d'organisation d'événements situées en Europe ou dans des pays tiers assurant un niveau de protection adéquat (sauf à mettre en place l'une ou l'autre des garanties appropriées prévues par la Réglementation applicable (Cf. Fiche n° 7 du guide *« Transferts internationaux »*).
- ✓ Ne pas enregistrer dans l'outil CRM des informations sensibles (exemples : informations révélant l'appartenance à une association politique ou religieuse…).
- ✓ Définir, le cas échéant, si les sponsors de l'événement sont autorisés à accéder à une liste de contacts et, dans l'affirmative :
- ✓ Veiller à ce que les participants soient informés de ce que les sponsors sont destinataires de certaines de leurs données personnelles lors de l'événement, pour quelles finalités et selon quelles conditions leurs données seront utilisées par ces derniers.
- ✓ Définir dans le contrat de sponsoring les usages autorisés des données relatives aux participants qui sont partagées (durée, interdiction de cession à des tiers, respect du droit d'opposition des contacts à recevoir des sollicitations commerciales de la part des sponsors, etc.).

Si votre cabinet intervient en qualité de sponsor, il faudra vérifier auprès de l'organisateur de l'événement s'il vous est permis d'accéder à des listes de participants, et les conditions d'utilisation des données les concernant.

1.2 Collecte de données publiques sur des réseaux sociaux professionnels

L'évolution des réseaux sociaux professionnels permet à toute entreprise d'avoir accès à une grande quantité d'informations sur de futurs prospects. Toutefois, et contrairement aux idées reçues, le fait que ces informations soient publiquement accessibles ne signifie pas que l'on puisse les collecter et les traiter en toute liberté.

[38] Au sens de la Réglementation applicable, voir Fiche n° 2 du guide *« Le statut du commissaire aux comptes »*.
[39] La CNIL et le G29 (CEPD) recommandent de faire figurer *a minima* lors de la collecte les informations suivantes :
– L'identité du responsable du traitement.
– Les détails de la finalité du traitement.
– Une description des droits des personnes concernées.

Ainsi, à titre d'exemple, la photographie de profil d'un contact sur un réseau social ne peut être importée et utilisée dans la base de contacts/l'outil CRM du cabinet ou dans un support de réunion, sans l'accord de la personne concernée.

La CNIL[40] considère que certaines collectes de données sur ces réseaux sociaux professionnels sont déloyales et illicites, dès lors que :

– la collecte est massive, répétitive et indifférenciée, **et**

– s'effectue sans en avertir les personnes concernées.

Il en va de même lorsque les données personnelles proviennent d'un site web dont les CGU interdisent l'extraction ou la réutilisation des données de ses utilisateurs à des fins commerciales. Ainsi, le réseau social professionnel LinkedIn prévoit dans ses conditions générales d'utilisation qu'il est interdit d'utiliser des procédés de *« web scraping »* des profils figurant sur le réseau social[41].

Pour en savoir plus, vous pouvez consulter la fiche de la CNIL sur la réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial.

• Les bonnes pratiques :

✓ S'équiper d'un outil permettant de centraliser la collecte de données personnelles à caractère professionnel et l'envoi de communications.

✓ Collecter/utiliser uniquement des données publiques pertinentes, sur des réseaux sociaux professionnels (principe de minimisation des données).

Par exemple : il est recommandé de se limiter aux informations suivantes : nom, prénom, titre/fonction, société, adresse email, téléphone, adresse professionnelle.

✓ S'abstenir de toute collecte massive de données à l'insu des personnes concernées (par exemple, collecte de plusieurs milliers de fiches contact sur un réseau professionnel).

✓ Informer les personnes concernées du traitement de leurs données par vos soins, *a minima* au moment de votre première communication avec eux.

Exemple de mention d'information

« Vos coordonnées figurent dans notre base de contacts. Si vous ne souhaitez pas recevoir de communications de notre part, veuillez-vous désinscrire ***(ici).*** *Si vous souhaitez que nous supprimions vos coordonnées de contact de notre base, veuillez-vous désinscrire* ***(ici).*** *Vous conservez la faculté d'exercer vos droits d'accès, de rectification, d'opposition et de suppression comme suit* ***[décrire la procédure]***. Pour plus d'informations sur notre politique de protection des données, veuillez cliquer ***(ici) [lien vers votre politique de confidentialité] ».***

[40] CNIL, Délibération du 21 septembre 2011, n° 2011-203 relative à la société Pages Jaunes : *« la circonstance que des profils personnels sont affichés publiquement sur Internet ne permet pas pour autant à un organisme tiers de procéder à une collecte massive, répétitive et indifférenciée de ces données sans en avertir les personnes concernées. Si les personnes concernées se sont inscrites sur des réseaux sociaux de leur plein gré, il ne résulte pas de cette démarche volontaire que l'ensemble de ces personnes ait également accepté, systématiquement et en toute conscience, que leurs informations soient récupérées par des tiers pour être agrégées à leurs données d'annuaires ».*

[41] Article 8.2 b) et m) des CGU de la plateforme LinkedIn au 06 janvier 2020 : *« Vous vous engagez à ne pas développer, prendre en charge ou utiliser des logiciels (…) ou tout autre moyen ou processus visant à effectuer du* web scraping *des Services ou à copier par ailleurs des profils et d'autres données des Services »*, et à ne pas *« utiliser de bots informatique ou d'autres méthodes automatisées afin d'accéder aux Services, ajouter ou télécharger des contacts ».*

• **Quelques exemples de ce qu'il ne faut pas faire :**

– Recourir à des solutions permettant l'extraction massive de données (Cf. point 1.2 ci-dessus).

– Multiplier les bases de contacts au sein du cabinet (ce qui rend difficile, voire impossible la gestion des droits d'opposition, Cf. Fiche n° 5 du guide *« Gestion des droits »*). Il est recommandé d'éviter au sein d'un même cabinet de tenir un fichier Excel par collaborateur/bureau.

– Créer de faux profils sur des réseaux sociaux pour accéder à des profils privés.

1.3 L'acquisition ou l'enrichissement de bases de données auprès de tiers

Vous pouvez être amenés à acquérir ou louer des bases de données de contacts auprès de tiers pour constituer ou enrichir votre propre base de prospects, soit de manière générale, soit pour un événement en particulier.

D'autres sociétés proposent également des services consistant à vérifier si vos bases de données sont exactes et à jour en croisant par exemple les données que vous détenez sur une personne concernée avec celles, publiques, relatives à cette même personne, ou à compléter votre base de données.

Vigilance ! Les sociétés qui proposent ces services peuvent avoir recours à plusieurs techniques, dont certaines reposent sur des algorithmes d'agrégation, d'extraction en masse de données ou encore qui permettent de deviner/reconstituer des informations, telles que des adresses électroniques, etc.

Par exemple : vous disposez du nom d'une personne et de sa société, le fournisseur se charge, grâce à ses outils, de « compléter les blancs » en retrouvant les adresses e-mail, numéros de téléphones portables, disséminés par ces personnes sur internet.

Certains procédés ou **outils technologiques** utilisés ne sont **pas conformes** aux exigences de la Réglementation applicable en ce qu'ils collectent les données des personnes à leur insu de manière déloyale et illicite.

Par exemple : la CNIL a considéré que la société les Pages Jaunes faisait une collecte illicite et déloyale de données personnelles en utilisant un logiciel de collecte automatique, dit *web crawler*, récupérant les données personnelles des utilisateurs de réseaux sociaux (Facebook, Twitter, Copains d'Avant, Linkedin, etc.) pour les associer aux informations classiques disponibles par l'annuaire du service Pages Blanches[42].

• **Les bonnes pratiques :**

✓ Obtenir la **garantie** auprès du vendeur / loueur de bases de données que les données des contacts y figurant ont été **collectées de manière loyale et licite** et que les personnes concernées ont été **informées** que leurs données personnelles seraient cédées à des tiers à des fins de prospection commerciale.

[42] CNIL, *délibération de la formation restreinte n° 2011-203 du 21 septembre 2011 portant avertissement à l'encontre de la société Pages Jaunes*

Exemple de clause de garantie

« Le fournisseur garantit que les données figurant dans sa base ont été collectées en conformité avec la Réglementation applicable en matière de protection des données personnelles et qu'elles peuvent être librement exploitées par le Client (Commissaire aux comptes) à des fins de prospection commerciale, les personnes concernées ayant été dûment informées que leurs données personnelles seraient cédées à des tiers pour être traitées à cette fin. Le fournisseur indemnisera et dégagera le Client de toute responsabilité en cas de demandes, actions ou recours de tiers (personnes concernées, autorités de protection des données…) relativement aux données ainsi [cédées/louées] ».

✓ Vous assurer que le vendeur fournit **des garanties appropriées** quant au respect de la Réglementation applicable en matière de protection des données personnelles (le cas échéant en concluant un accord/une annexe sur la protection des données personnelles) :

- la base ne contient pas de données sensibles (sauf autorisation légale spécifique) **(principe de minimisation)** ;
- les personnes concernées ont été informées de la possibilité d'une transmission de leurs informations à des tiers **(principes de loyauté, licéité et transparence)** ;
- les personnes concernées ont été informées de la possibilité de s'opposer au traitement de leurs données à des fins de prospection **(principes de transparence et limitation des finalités)**.

✓ Vous assurer que la base de données est régulièrement tenue à jour **(principe d'exactitude)**.

✓ Informer les personnes concernées, *a minima* au moment de votre première communication avec eux, des traitements que vous opérez (voir par exemple le modèle de mention d'information proposé au ci-dessus).

✓ Lorsque les conditions sont réunies, réaliser une analyse d'impact avant la mise en œuvre du traitement pour s'assurer qu'il est respectueux du RGPD. Un logiciel *open source* est mis à votre disposition par la CNIL pour faciliter la réalisation d'analyse d'impact[43].

• Quelques exemples de ce qu'il ne faut pas faire :

- Recourir à des prestataires de services **utilisant des méthodes de collecte déloyales**, telles que le *« scraping »* : la collecte des données n'est pas faite de manière transparente et loyale, les personnes concernées ignorent le plus souvent que leurs données figurent dans de telles bases de données et l'exercice de leurs droits n'est pas effectivement mis en œuvre.
- Transférer à des tiers les données de vos prospects à d'autres fins que celles prévues initialement sans avoir informé au préalable la personne concernée de l'existence d'éventuels transferts à des destinataires identifiés.

[43] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

1.4 La collecte de données *via* votre site internet (cookies et formulaire de contact)

Formulaire de contact figurant sur votre site internet

Dans le cas où vous mettez en place des formulaires de contact sur votre site internet pour l'envoi de *newsletters* ou la prise de contact pour des questions diverses, vous pouvez être amenés à collecter les informations telles que les nom, prénom, adresse e-mail, titre/fonction d'une personne.

Dès lors, vous devrez faire figurer une mention d'information au niveau de ces formulaires de collecte (Cf. Fiche n° 4 du guide *« Transparence – Information »*).

Cookies et autres traceurs

L'utilisation de traceurs pour collecter des données de navigation des visiteurs de votre site internet est possible dans la limite des recommandations édictées par la CNIL. Pour plus d'informations, vous pouvez vous référer aux lignes directrices de la CNIL relatives aux opérations de lecture ou écriture dans le terminal d'un utilisateur ainsi qu'aux Recommandations de la CNIL *« Cookies et traceurs »*.

Vous devrez mettre en place un bandeau d'information relatif à l'utilisation de vos cookies permettant aux utilisateurs d'être informés et d'accepter ou de refuser individuellement chaque finalité et notamment celles relatives à la prospection commerciale et au partage des données avec des tiers et partenaires (Cf. exemple de mention d'information relative aux cookies Fiche n° 4 du guide *« Transparence – Information »*). Selon la CNIL, en cas de refus, l'utilisateur doit pouvoir continuer la navigation sur le site web, et la poursuite de navigation ne peut être interprétée comme un consentement valable.

2. Étape 2 – L'entrée en relation d'affaires avec un client : connaître son client (KYC) dans le cadre de la lutte contre le terrorisme et le blanchiment de capitaux

Dans le cadre de vos obligations en matière de lutte contre le terrorisme et le blanchiment de capitaux, vous êtes amené à collecter un certain nombre d'informations spécifiques relatives à vos clients au titre du processus communément désigné sous l'acronyme « KYC » ou *« Know Your client »*[44].

En effet, conformément à l'article L. 561-5-1 du Code Monétaire et Financier, les commissaires aux comptes sont tenus de recueillir les informations relatives à l'objet et à la nature de leur relation d'affaires avec leur client (entité contrôlée) et tout autre élément d'information pertinent. Ils actualisent ces informations pendant toute la durée de la relation d'affaires.

[44] Article L. 561-5-1 du Code monétaire et financier (CMF) : *« Avant d'entrer en relation d'affaires, les personnes mentionnées à l'article L. 561-2 recueillent les informations relatives à l'objet et à la nature de cette relation et tout autre élément d'information pertinent. Elles actualisent ces informations pendant toute la durée de la relation d'affaires ».*

Quelles sont les implications pratiques ?

2.1 Informer ses clients

Normalement, ces traitements doivent être mentionnés dans vos lettres de mission et/ou votre politique de confidentialité (Cf. Fiche n° 4 du guide *« Transparence – Information »* et cf. Modèle de lettre de mission établi par la CNCC).

2.2 Quelles catégories de données collecter ?

Il ne faut pas tomber dans l'écueil de collecter trop de données personnelles (principes de minimisation et de pertinence des données) et vous devez vous assurer que les données collectées sont adaptées au regard de la finalité poursuivie (principe de proportionnalité).

Conservation de la copie de la carte nationale d'identité : quelles sont les contraintes à respecter ?

Au titre de ses obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, le commissaire aux comptes doit *« identifier le client et, le cas échéant, le bénéficiaire effectif (…) » et « vérifier ces éléments d'identification sur présentation de tout document écrit à caractère probant »*[45].

Lorsque le commissaire aux comptes vérifie l'identité d'une personne physique (représentant légal d'un client par exemple), il peut le faire (i) soit par la présentation, par cette dernière, de l'original d'un document officiel en cours de validité, (ii) soit par la prise d'une copie de ce document, afin de noter, *a minima*, les nom, prénoms, date et lieu de naissance de la personne, ainsi que la nature, les date et lieu de délivrance du document consulté et les nom et qualité de l'autorité ayant délivré ce document[46].

Par ailleurs, conformément à la **norme d'exercice professionnel n° 9605** relative aux obligations du commissaire aux comptes en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme[47], le commissaire aux comptes **est tenu de vérifier les éléments d'identification du bénéficiaire effectif sur présentation d'un document écrit à caractère probant.**

À ce titre, **vous pouvez demander une copie d'un document officiel** en cours de validité comportant la photographie du client personne physique, mentionnant ses nom et prénom ainsi que ses date et lieu de naissance. Il peut s'agir par exemple de la copie de la carte d'identité ou du passeport[48].

Si les dispositions légales susmentionnées n'imposent pas la conservation de la pièce d'identité, la norme d'exercice professionnelle susmentionnée précise que :

- *« Le commissaire aux comptes conserve dans ses dossiers les documents et informations, quel qu'en soit le support, permettant de justifier des mesures de vigilance mises en œuvre et de leur adéquation au risque de blanchiment des capitaux et de financement du terrorisme »* **(§ 73)** ; et

[45] Article L. 561-5 du Code Monétaire et Financier (CMF)
[46] Article R. 561-5-1 du CMF issu du décret n° 2020-118 du 12 février 2020
[47] NEP-9605 publiée le 24 octobre 2019 et homologuée le 3 novembre 2019
[48] NEP-9605 publiée le 24 octobre 2019 et homologuée le 3 novembre 2019 **(§ 19)**

– *« Le commissaire aux comptes conserve **pendant cinq ans** à compter de la fin du mandat de commissariat aux comptes, de la mission ou de la prestation les documents et informations relatifs à l'identification et à la vérification des éléments d'identification du client, ou du client occasionnel, et le cas échéant, du bénéficiaire effectif »* (**§ 74** NEP-9605 et article L. 561-12 du CMF).

Ce que dit la CNIL[49] sur les vérifications d'identité :

> *« Si l'organisme doit s'assurer de l'identité d'une personne avant d'entrer en relation commerciale avec elle, la simple présentation d'un justificatif peut suffire.*
>
> *Une copie de ce justificatif peut être conservée pour une durée de 6 ans lorsque la loi le prévoit ou si l'organisme justifie en avoir besoin pour se pré-constituer une preuve en cas de contentieux.*
>
> *Dans ce cas, des **mesures de sécurité renforcées**, telles que par exemple la limitation de la qualité de l'image numérisée ou l'intégration d'un filigrane comportant la date de collecte et l'identité de l'organisme, doivent être mises en œuvre afin de lutter contre les risques de mésusage de ces informations, en particulier l'utilisation des photographies à des fins de reconnaissance faciale. »*

Par conséquent, le commissaire aux comptes est autorisé, s'il l'estime nécessaire, à conserver une copie de ce justificatif, pendant une durée limitée et en adoptant des mesures de sécurité renforcées (Cf. Fiche n° 8 du guide *« Gestion de la sécurité des données »*).

Néanmoins, s'il n'est pas envisageable de mettre en place ce type de mesures de sécurité renforcées, il est recommandé de ne pas conserver la copie de ce justificatif après avoir opéré les vérifications d'usage. Ceci implique de supprimer cette pièce dans toute la chaine de collecte et transmission de la pièce (suppression du fichier figurant sur une clé USB, dans le dossier de travail, en pièce jointe de l'e-mail adressé par le client…).

2.3 Quelle est la durée de conservation recommandée de ces informations ?

La durée de conservation des données collectées au titre du KYC doit être documentée au sein du Registre au titre de l'article 30 du RGPD.

La norme d'exercice professionnelle **NEP-9605** précise que *« les documents et informations relatifs à l'identité du client, ou du client occasionnel, et le cas échéant, du bénéficiaire effectif ainsi que les autres éléments d'information nécessaires, sont conservées **pendant cinq ans à compter de la fin du mandat de commissariat aux comptes, de la mission ou du service »***.

> *À noter :* un modèle de fiche de traitement spécifique au traitement KYC, destinée à intégrer le registre des activités de traitement, figure en annexe de la présente fiche.

[49] Projet de Référentiel CNIL, https://www.cnil.fr/sites/default/files/atoms/files/referentiel-gestion-commerciale.pdf ; et Délibération CNIL 2018-051 du 15 février 2018

Pour traiter des intérêts potentiellement divergents entre l'obligation d'instruction KYC du commissaire aux comptes et la protection de la vie privée des personnes concernées, **une logique d'arbitrage interne** devra être mise en place et des règles devraient être précisées concernant les habilitations, l'utilisation possible des données, le partage de données, leur conservation, etc.

Par exemple : l'article L. 511-34 du Code monétaire et financier permet le partage des données intra groupe (sous certaines conditions) lorsque les informations sont nécessaires à l'organisation de la lutte contre le blanchiment de capitaux et contre le financement du terrorisme.

Pour en savoir plus : CNIL, Norme Simplifiée NS-003 concernant les traitements mis en œuvre par des organismes financiers relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi qu'à l'application des sanctions financières.[50]

3. Étape 3 – La gestion de la relation d'affaires avec ses clients

Cette étape ne présente pas de spécificité propre à la profession. L'on rappellera néanmoins quelques principes.

3.1 Rappel des principes

S'agissant de la gestion des clients et prospects, la CNIL[51] rappelle que le responsable du traitement doit :

- **Informer** ses clients et prospects des conditions dans lesquelles il traite leurs données et de leurs droits (Cf. Fiche n° 4 du guide *« Transparence – Information »*).
- **Minimiser** les données collectées : il s'agit de ne collecter et traiter que les informations nécessaires à la gestion de la relation commerciale (données professionnelles, telles que nom, prénom, numéro de téléphone professionnel, société, fonction, éventuellement photographie du profil professionnel, etc.), y compris s'agissant des procédures KYC *(Know Your Client)*.
- **Prévoir des mesures de sécurité** adaptées au regard des risques.
- **Limiter la durée de conservation des données.** Des obligations légales peuvent imposer de conserver certaines données pendant un temps donné.
- **Demander conseil et assistance**, le cas échéant, au Délégué à la protection des données (DPO).

[50] À la suite de l'entrée en application du RGPD, les normes simplifiées adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

[51] CNIL, Gestion des clients et prospects : que faire ? Pour en savoir plus, vous pouvez consulter le projet de référentiel de la CNIL « Gestion commerciale », qui encadre les traitements les plus courants (hors détection et prévention de la fraude, enrichissement des bases de données à partir d'information collectées par des tiers).
https://www.cnil.fr/sites/default/files/atoms/files/referentiel-gestion-commerciale.pdf

– **Documenter** les traitements au sein du registre des activités de traitement tenu par le responsable du traitement (Cf. Fiches n° 1 « *Gouvernance et Accountability* » du guide et ses Annexes, ainsi que l'Annexe 1 de la présente Fiche n° 3 « *Fiche de Traitement KYC* »).

3.2 Du bon usage de votre outil de gestion de relation commerciale (CRM)

De plus en plus de sociétés se dotent d'outils CRM afin d'optimiser et gérer au mieux leurs relations d'affaires avec leurs contacts.

• **Les bonnes pratiques consistent à :**

✓ Privilégier les solutions CRM qui sont « *Privacy by design*»[52] et permettent notamment, de contrôler les durées de conservation des données personnelles, d'identifier aisément les préférences des clients (en matière de réception de communications commerciales par exemple), de faire valoir efficacement leur droit d'opposition…

✓ Renforcer le niveau de sécurité des données selon le type de données personnelles collectées, en particulier dans le cadre du traitement des informations recueillies au titre du processus KYC évoqué ci-avant (voir point 2 ci-avant).

✓ Vérifier s'agissant des solutions CRM en ligne (hébergement cloud, mode SaaS, solutions mutualisées en ligne) :

- la nationalité de l'éditeur (notamment si l'éditeur est américain, il peut être soumis au *Cloud Act*) ;
- que le lieu d'hébergement est situé dans un pays offrant un niveau de protection adéquat des données ;
- si des intervenants localisés dans des pays n'offrant pas un niveau de protection adéquat ont accès aux données ;

et, le cas échéant, mettre en œuvre l'une ou l'autre des garanties prévues par la Réglementation applicable (signature de clauses contractuelles type approuvées par l'Union européenne, règles d'entreprises contraignantes…). (Cf. Fiche n° 7 « *Transferts internationaux de données* »).

✓ Ne pas succomber à la tentation de collecter trop d'informations sur ses contacts (principes de minimisation, pertinence), quand bien même l'outil CRM dispose d'une multitude de fonctionnalités attrayantes, mais qui ne sont pas conformes à l'esprit ni à la lettre de la Réglementation applicable.

✓ Limiter et contrôler les champs de commentaires libres, sensibiliser les utilisateurs sur la pertinence des informations renseignées dans ces champs.

La CNIL[53] a ainsi sanctionné un organisme de formation après avoir constaté que les zones de commentaires libres incluaient des insultes, des informations sur la santé des parents et des élèves, sur la vie privée des élèves et de leurs proches, etc.

[52] CNIL « Guide du développeur », la CNIL propose des recommandations pour les développeurs dans l'élaboration de leurs solutions.
[53] Délibération n° 2010-113 du 22 avril 2010 de la formation restreinte portant avertissement à l'encontre de la société X exerçant sous l'enseigne Y

Afin de sensibiliser vos collaborateurs sur le sujet, il est notamment recommandé de (i) les former, (ii) réaliser régulièrement un audit/une revue des informations figurant dans les zones de commentaires libres de vos outils CRM, ainsi que (iii) des points de sensibilisation sur les règles d'utilisation des zones libres (dans votre charte informatique, ou dans une charte de bonne conduite *ad hoc*).

3.3 Communiquer avec ses clients et prospects

Dans le cadre d'opérations de « prospection commerciale », les recommandations générales de la CNIL s'appliquent aux commissaires aux comptes[54].

Le commissaire aux comptes opérant le plus souvent dans le cadre de rapports entre professionnels *(B to B)* il n'est pas nécessaire qu'il obtienne le consentement de ses contacts pour leur adresser des communications commerciales.

Cette dispense est valable pour autant que les contacts ont reçu au moment de la collecte une **information préalable** sur la possibilité de recevoir de telles communications et qu'ils puissent s'y opposer facilement.

> *À noter :* les adresses professionnelles génériques de type <info@nomsociete.fr> et <contact@nomsociete.fr> sont des coordonnées de personnes morales ; elles ne sont pas soumises aux principes du consentement et du droit d'opposition.

• Les bonnes pratiques à mettre en place :

- ✓ Informer vos contacts de la possibilité que leurs coordonnées de contact soient utilisées à des fins de sollicitation professionnelle (Cf. Fiche n° 4 du guide *« Transparence – Information »*).
- ✓ Permettre aux destinataires de s'opposer à l'utilisation de leurs données à des fins de sollicitation professionnelle.
- ✓ Par exemple : insertion d'un lien dans les mailings, permettant de se désinscrire facilement d'une liste de diffusion.
- ✓ Tenir à jour une liste d'opposition.

4. Étape 4 : La fin de la relation d'affaires – quelles durées de conservation ?

4.1 Durée de conservation des données de prospects

Les données personnelles relatives à **un prospect** non-client peuvent être conservées pendant un délai de 3 ans à compter de leur collecte par le responsable du traitement (et sous réserve de l'exercice de son droit de suppression de ses données à tout moment) ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un

[54] https://www.cnil.fr/fr/la-prospection-commerciale-par-courrier-electronique

clic sur un lien hypertexte contenu dans un courriel ; en revanche, la seule ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect)[55].

À l'issue de ce délai de 3 ans, le responsable du traitement devra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales et, à défaut de réponse, supprimer ses coordonnées.

En cas d'exercice du droit d'opposition, ces données peuvent être archivées pendant un délai de 3 ans[56].

La gestion des **listes d'opposition** à recevoir de la prospection commerciale. Lorsqu'une personne exerce son droit d'opposition à recevoir des communications commerciales, les informations permettant de prendre en compte son droit d'opposition doivent être conservées au minimum 3 ans à compter de l'exercice du droit d'opposition. Ces données ne peuvent en aucun cas être utilisées à d'autres fins que la gestion du droit d'opposition et seules les données nécessaires à la prise en compte du droit d'opposition doivent être conservées (par exemple, l'adresse électronique).

4.2 Durée de conservation des données clients

Les données clients ne peuvent pas être conservées indéfiniment et ne doivent pas être supprimées trop tôt.

Les données traitées à des fins de sollicitation professionnelle

Les données personnelles collectées à des fins commerciales ne peuvent pas être conservées au-delà de la **durée strictement nécessaire à la gestion de la relation commerciale**.

Par exemple : il peut s'agir ici des informations relatives à l'identité de vos contacts clients, aux moyens de paiement, au règlement des factures, figurant notamment au sein de votre CRM, sur vos factures, etc.

Les données personnelles des clients utilisées à des fins de sollicitation professionnelle peuvent être conservées pendant **un délai de trois ans** à compter de la fin de la relation commerciale.

Par exemple : la fin de la relation commerciale peut être constituée à compter du terme d'une lettre de mission ou du dernier contact émanant du client.

Les données traitées à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme (KYC)

S'agissant des informations collectées conformément à l'obligation légale imposée au commissaire aux comptes de lutter contre le blanchiment de capitaux et le financement du terrorisme (Loi Sapin II), notamment à travers le processus d'investigation KYC, **vous devez les conserver pendant 5 ans à compter de la fin du mandat de commissariat aux comptes, de la mission ou du service**[57].

[55] CNIL, Norme Simplifiée NS-048 concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et prospects

[56] Article 8 du Code de procédure pénale

[57] *« Le commissaire aux comptes conserve les documents et informations relatives à l'identité du client, ou du client occasionnel (…)* ***pendant 5 ans*** *à compter de la fin du mandat de commissaire aux comptes, de la mission ou du service »* (§ 58 NEF-9605 et article L. 561-12 du CMF).

Au terme de ce délai de 5 ans vous devrez soit (i) supprimer les informations collectées à cette fin, soit (ii) le cas échéant, mettre en place une politique d'archivage des données avec accès restreint (voir point 4.3 ci-après).

4.3 Mise en place d'une politique d'archivage (prolongation de la durée de conservation)

Il peut être justifié que les données personnelles soient conservées pour des durées plus longues en archivage intermédiaire distinct de la base active, avec accès restreint dans la mesure où ces données présentent **un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables**, notamment en matière commerciale, civile et fiscale.

Pour pouvoir conserver, au-delà de la durée de conservation fixée par la loi, des informations relatives à des clients ou des prospects à des fins d'analyses ou d'élaboration de statistiques agrégées, les données **doivent être anonymisées de manière irréversible**, en procédant à la purge de toutes les données à caractère personnel, y compris les données indirectement identifiantes[58].

Pour en savoir plus sur la conservation et l'archivage Cf. Fiche n° 8 du guide *« Sécurité des données »*.

Plus particulièrement, les données permettant d'établir la preuve d'un droit ou d'un contrat, ou conservées au titre du respect d'une obligation légale, **peuvent faire l'objet d'une politique d'archivage intermédiaire pour une durée n'excédant pas la durée nécessaire aux finalités pour lesquelles elles sont conservées**, conformément aux dispositions en vigueur (notamment mais non exclusivement celles prévues par le Code de commerce et le Code civil). Il convient de prévoir à cet effet **une base de données d'archives dédiée ou une séparation logique dans la base de données active**, après avoir opéré un tri des données pertinentes à archiver.

Pour en savoir plus : CNIL, Norme Simplifiée NS-048 concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et prospects[59].

Par exemple : tout commissaire aux comptes est tenu par une obligation de conservation particulière pendant **six ans** des dossiers et documents établis au titre de ses missions énoncées à l'article R. 823-10 du Code de commerce, même après la cessation de ses fonctions[60].

Pour en savoir plus sur les durées de conservations liées à certains traitements propres au commissaire aux comptes : Cf. Annexe 1 de la Fiche n° 1 du guide *« Gouvernance et accountability »*.

[58] Le G29 a adopté un avis le 10 avril 2014 sur les techniques d'anonymisation.
[59] Suite à l'entrée en application du RGPD, les normes simplifiées adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.
[60] Article R. 821-68 du Code de commerce

Annexe 1 – Fiche de traitements CAC relative au KYC à insérer au registre art. 30 RGPD
Modèle de fiche de traitements CAC relative au KYC

Traitement de données à caractère personnel propre au KYC		
N°/REF		
Date de création du traitement		
Dernière mise à jour		
Application(s)/logiciels concernée(s)	Nom de l'application/du logiciel : Nom de l'éditeur :	Commentaires :
Acteurs du traitement		
Responsable du traitement de données à caractère personnel*	Nom :	Coordonnées *(adresse postale, email, tél)* :
Délégué à la protection des données*	Nom : Société du DPO (si DPO externe) :	Cordonnées *(adresse postale, email, tél)* :
Représentant légal du responsable du traitement	Nom :	Cordonnées *(adresse postale, email, tél)* :
Responsable(s) conjoint(s)	Nom :	Coordonnées *(adresse postale, email, tél)* :
Sous-traitant *(à décliner en autant de sous-traitants)*	Nom :	Coordonnées *(adresse postale, email, tél)* :
Destinataire(s)*	1. Au sein du personnel habilité des responsables de traitement : – les personnes en relation avec la clientèle et les gestionnaires de contrat et de sinistres pour les clients dont ils ont la charge à l'exception des informations relatives aux déclarations de soupçon ; – les personnes habilitées à prendre la décision de nouer ou de maintenir une relation d'affaires avec une PPE ; – le personnel habilité du (ou des) service(s) chargé(s) de la lutte contre le blanchiment, notamment ceux ayant la qualité de correspondant ou de déclarant Tracfin, au sein des services de contrôle, d'audit ou juridique de l'organisme responsable du traitement. 2. Parmi les autorités compétentes : – la cellule de renseignement financier Tracfin du ministère de l'Économie, des Finances et de l'Industrie ; – les autorités de contrôle compétentes au sens de l'article L. 561-36 du CMF ; – pour les données relatives aux personnes qui font l'objet d'une mesure de gel des avoirs, la Direction générale du Trésor ;	

Traitement de données à caractère personnel propre au KYC	
	– les autorités de contrôle compétentes des autres états membres de la Communauté européenne, des états partie à l'accord sur l'Espace économique européen et des états où sont applicables les accords conclus avec l'Autorité de Contrôle Prudentiel ou l'Autorité des Marchés Financiers en application des dispositions prévues aux articles L. 632-7, L. 632-13 et L. 632-16 du CMF. 3. Parmi les autres organismes financiers – dans le respect des conditions posées au II de l'article L. 561-7 du CMF, les personnes assujetties aux obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme mentionnées aux 1° à 7° de l'article L. 561-2 du CMF (ci-après « autres organismes ») ; – dans le respect des conditions posées à l'article L. 561-20 du CMF, les personnels habilités des autres organismes au sens du paragraphe précédent, les compagnies financières et les compagnies financières holding mixtes, lorsqu'ils appartiennent à un même groupe tel que défini au III de l'article L. 511-20 du CMF ou à l'article L. 334-2 du Code des assurances, en ce qui concerne l'existence et le contenu de la déclaration de soupçon ; – dans le respect des conditions posées à l'article L. 561-21 du CMF, les autres organismes au sens du premier paragraphe, qui interviennent pour le même client dans la même transaction, en ce qui concerne l'existence et le contenu de la déclaration de soupçon.
Finalités du traitement*	
Finalité	Lutte contre le blanchiment de capitaux et le financement du terrorisme.
Sous-Finalité 1	Mise en œuvre des obligations de vigilance à l'égard de la clientèle conformément à l'approche par les risques.
Sous-Finalité 2	Recherche des personnes qui doivent faire l'objet de mesures de vigilance complémentaires en tant que personnes politiquement exposées (PPE) au sens de l'article R. 561-18 du CMF et des personnes susceptibles de faire l'objet de mesures de vigilance renforcées.
Sous-Finalité 3	Déclenchement des alertes et déclarations de soupçon.
Sous-Finalité 5	Application des mesures de gel des avoirs dans le cadre de la lutte contre le financement du terrorisme et des sanctions financières.
Base juridique associées au traitement	
Obligation légale à laquelle le responsable du traitement est soumis :	Obligations légales et règlementaires relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (art. L. 561-1 et suivants et R. 561-1 et suivants du Code Monétaire et Financier).

Traitement de données à caractère personnel propre au KYC		
Catégories de personnes concernées*		
1. Personnel de l'entité contrôlée (dirigeants, salariés, stagiaires…). 2. Actionnaires et mandataires de l'entité contrôlée. 3. Toute partie prenante de l'entité contrôlée (prestataires, clients de l'entité auditée, fournisseurs…). 4. Toutes personnes ayant sollicité la conclusion d'un contrat ou la réalisation d'une opération. 5. Clients personnes physiques, qu'ils soient habituels, ou occasionnels. 6. Tous tiers concernés par les opérations financières des clients, et/ou tous tiers hébergeant des clients. 7. Toutes personnes physiques représentant des personnes morales. 8. Tous bénéficiaires effectifs. 9. Toutes personnes susceptibles d'être classées dans la catégorie des personnes politiquement exposées conformément aux dispositions de l'article R. 561-18 du Code monétaire et financier. 10. Toutes personnes mentionnées sur les listes de gel des avoirs ou de sanctions financières. 11. L'identité, l'activité et les coordonnées professionnelles du (ou des) déclarant (s) et correspondant(s)Tracfin peuvent également être mentionnées dans le traitement.		
Catégories de données traitées et durées de conservation **Rappel AU 003 :** À l'exception des données relatives à l'identification et au justificatif de domicile, la collecte des informations ci-dessous avant l'entrée en relation ou au cours de celle-ci n'est pas systématique et indifférenciée pour l'ensemble des personnes concernées. Elle doit s'avérer nécessaire à l'évaluation du risque présenté par le client, l'opération demandée ou le contrat souscrit et être proportionnée à la classification des risques de l'établissement financier élaborée *ab initio* par grandes catégories de client, de produit et de contrat. Des données et pièces justificatives complémentaires peuvent également être collectées directement auprès de la personne concernée en cas de risque élevé ou d'opérations complexes, d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite.		
Données d'identification	**Pour les personnes physiques :** Nom, prénom, code état (M., Mme, Mlle), pseudonyme(s), date et lieu de naissance, genre, nationalité, langue natale, une copie d'un ou plusieurs documents officiels en cours de validité comportant sa photographie, le relevé des mentions suivantes : nature, date et lieu de délivrance du ou des documents et les nom et qualité de l'autorité ou de la personne qui a délivré le ou les documents et, le cas échéant, l'a ou les a authentifiés.	5 ans à compter de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).

Traitement de données à caractère personnel propre au KYC		
	Pour les personnes physiques représentant des personnes morales : mandats et pouvoirs, identité des dirigeants, associés et mandataires, copie de tout acte ou extrait de registre officiel datant de moins de trois mois constatant l'identité des associés et dirigeants sociaux mentionnés aux 1° et 2° de l'article R. 123-54 du Code de commerce ou de leurs équivalents en droit étranger.	
Données de contact/ coordonnées	Adresse et justificatif d'adresse du domicile personnel à jour au moment où les éléments sont recueillis, et coordonnées de contacts personnelles et/ou professionnelles : email, adresse postale, téléphone, fax, Messenger.	5 ans à compter de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).
Données de situation professionnelle, économique et financière	Catégorie socioprofessionnelle, Code NAF, profession, nom de l'employeur, nature et niveau des revenus ou du chiffre d'affaires, justificatifs d'activité économique, de ressources ou de patrimoine prenant la forme d'un engagement sur l'honneur de la personne concernée ou d'un justificatif de nature à démontrer la véracité des informations déclarées.	5 ans à compter de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).
Données relatives au patrimoine	Éléments permettant d'apprécier le patrimoine.	5 ans à compter de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).
Données judiciaires	Infractions et condamnations (motifs, date, sanctions…).	5 ans à compter de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).
Données relatives à des déclarations de soupçon	Existence et contenu.	5 ans à compter de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).
Transfert de données vers un pays tiers à l'UE ou vers une organisation internationale* [Oui/ Non]		

Traitement de données à caractère personnel propre au KYC		
Si oui, organisme destinataire	Nom de l'outil / du sous-traitant : Pays : Type de garanties :	Type de garantie mise en œuvre : *(Clauses contractuelles types, BCR en cas de transferts au sein d'un réseau de commissaire aux comptes…).*
Mesures de sécurité techniques/ organisationnelles*	Mesures de sécurité techniques Mesures de sécurité organisationnelles Mesures de sécurité physiques *(faire référence aux politiques/guides de sécurité).*	
Information des personnes concernées	L'information des salariés, actionnaires, mandataires et parties prenantes de l'entité contrôlée n'est pas obligatoire (cf. Art. 14, 5°d. du RGPD). Le commissaire aux comptes informe l'entité contrôlée des traitements réalisés dans le cadre de ses obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme dans sa lettre de mission et sa politique de confidentialité. Le personnel du cabinet du commissaire aux comptes est informé des traitements réalisés *via* ***[à adapter : la charte informatique, politique de confidentialité, contrat de travail…]***.	
Analyse d'impact relative à la protection des données		
Nécessaire ?	**Oui** L'article 35 du RGPD dispose que le responsable du traitement effectue une analyse d'impact lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. L'article 35 § 3 du RGPD énonce les 3 principaux cas dans lesquels une analyse d'impact est nécessaire : 1. Évaluation systématique et approfondie d'aspect personnel fondé sur un traitement automatisé. 2. Traitement à grande échelle de catégories particulières de données. 3. Surveillance systématique à grande échelle d'une zone accessible au public. Le Comité Européen de la Protection des Données (CEPD) a complété cette liste dans ses lignes directrices relatives à l'analyse d'impact. Lorsque 2 des 9 critères énoncés sont remplis, le traitement nécessite d'être soumis à une analyse d'impact. Le présent traitement remplit au moins les critères suivants : – Évaluation ou notation (le CEPD cite expressément comme exemple les obligations LBC/FT – page 10). – Traitement à grande échelle de données relatives à des faits susceptibles de qualification pénale.	

Traitement de données à caractère personnel propre au KYC	
	En revanche, l'article 35 § 10 précise que les § 1 à 7 de l'article 35 (Études d'Impact) ne sont pas applicables *« lorsque le traitement est effectué en application de l'article 6, paragraphe 1 point c) ou e)* [obligation légale et intérêt légitime], *a une base juridique dans le droit […] de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question ».* Le Comité Européen de la Protection des Données (CEPD) précise dans ses lignes directrices relatives à l'analyse d'impact que *« Dans le cas d'une AIPD réalisée au stade de l'élaboration de la législation conférant une base juridique au traitement, un réexamen pourra être nécessaire avant le lancement des opérations, la législation adoptée étant susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données »* (page 15). **Une analyse d'impact relative à la protection des données n'ayant pas été réalisée dans le cadre de l'adoption de la réglementation encadrant la lutte contre le blanchiment de capitaux** et le financement du terrorisme, **la réalisation d'une analyse d'impact par le responsable du traitement est – en l'état – nécessaire**[61].

[61] Pour cela, vous pouvez utiliser le logiciel *open source* mis à votre disposition par la CNIL : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Annexe 2 – Tableau de synthèse des bases légales et durées de conservation applicables à la gestion de la relation professionnelle avec vos clients et prospects

FINALITÉS	BASE LÉGALE i.e. ce qui vous autorise à traiter les données	DURÉES DE CONSERVATION
Gestion des contrats / missions		
Suivi de la mission	**Respect d'une obligation légale (Certification des comptes, SACC légaux) ou Intérêt légitime[62].**	Durée de la relation contractuelle (de la lettre de mission ou du dernier contact avec le client).
Obligations comptables, fiscales, etc.	Respect d'une obligation légale de conservation des données. (obligation de s'assurer de l'identité de la personne en demandant la fourniture d'un justificatif d'identité).	Sous la forme d'archive intermédiaire : durée légale de conservation (obligation comptable de 10 ans).
Gestion des pré-contentieux et contentieux	Intérêt légitime de l'organisme pour l'établissement de la preuve d'un droit ou d'un contrat (p. exemple : en cas de contentieux).	Durée de la prescription (civile, commerciale, etc.).
Opérations de sollicitation et communication		
Par voie électronique (en vue de l'envoi de courriel, SMS, automate vocal, etc.) – hors rapport entre professionnels	Consentement de la personne concernée.	Jusqu'au retrait du consentement ou 3 ans à compter du dernier contact.
Par voie postale ou intervention humaine	Intérêt légitime du commissaire aux comptes[63].	
À destination de professionnels		
Pour des biens et services analogues		
Gestion d'une liste d'opposition	Intérêt légitime du commissaire aux comptes.	3 ans à compter de l'exercice du droit.

[62] L'exécution du contrat ne semble pas pouvoir être une base légale possible dans la mesure où selon l'article 6, § 1, (b) du RGPD il est nécessaire que la personne concernée soit partie au contrat. Ce qui n'est pas le cas dans le cadre d'une lettre de mission entre un commissaire aux comptes et son client. Les personnes concernées ne sont pas partie à ladite lettre de mission.

[63] CNIL, L'intérêt légitime : comment fonder un traitement sur cette base légale ?

FINALITÉS	BASE LÉGALE i.e. ce qui vous autorise à traiter les données	DURÉES DE CONSERVATION
Traçage / suivi de la navigation des personnes	Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la LIL modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traces	
Cookies et autres traceurs	• **Consentement** spécifique pour chaque finalité de traceurs. • **Exception au consentement :** si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur : – a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; ou – est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur. – Les cookies de mesure d'audience tels que décrits aux points 50 à 52 de la Délibération n° 2020-091.	• **Pour le consentement** : jusqu'à l'exercice du retrait du consentement. • **Pour les traceurs de mesure d'audience :** – Les traceurs ne doivent pas avoir une durée de vie excédant **13 mois et cette durée ne doit pas être prorogée** automatiquement lors des nouvelles visites. – **25 mois** pour les données collectées grâce à ces traceurs (conformément aux recommandations de la CNIL dans sa Délibération n° 2020-092 du 17 septembre 2020).
La lutte contre le blanchiment de capitaux et le financement du terrorisme		
Mise en œuvre des obligations de vigilance à l'égard de la clientèle (investigation KYC, etc.)	Obligation légale[64] (art. L. 561-1 et suivants, et R. 561-1 et suivants du Code monétaire et financier).	5 ans à compter de la clôture de leur compte ou de la cessation de la relation avec le client (art. L. 561-12, Code monétaire et financier).

[64] Pour en savoir plus, voir la note d'information de la CNIL relative à « L'obligation légale : dans quels cas fonder un traitement sur cette base ? »

Transparence

Transparence

Fiche n° 4

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

Cette fiche a pour objectif de vous guider dans la mise en œuvre de l'obligation d'information qui vous incombe en tant que responsable du traitement.

En vertu du principe de transparence, le responsable du traitement est tenu d'informer les personnes concernées du traitement de leurs données personnelles, de ses modalités et des droits dont elles disposent.

Pour être conforme à l'exigence de transparence, l'information fournie aux personnes concernées doit être claire, concise et contenir *a minima* les éléments énumérés aux articles 13 ou 14 du RGPD, selon que les données sont collectées directement auprès de la personne concernée (article 13) ou indirectement (article 14). Ces éléments couvrent essentiellement :

- L'identité et les coordonnées du **responsable du traitement**.
- Les **coordonnées du délégué à la protection des données** le cas échéant.
- Les **finalités** du traitement.
- La **base juridique** du traitement.
- Les **destinataires** ou catégories de destinataires des données personnelles.
- La **durée de conservation** des données personnelles (du moins les critères utilisés pour déterminer cette durée).
- **Les droits** dont dispose la personne concernée, y compris celui d'introduire une réclamation auprès de la CNIL.

Les données personnelles traitées par le commissaire aux comptes dans le cadre de ses missions sont presque essentiellement collectées de **manière indirecte** (transmises par l'entité contrôlée ou contenues dans des documents transmis par l'entité contrôlée).

En cas de collecte indirecte, **le commissaire aux comptes bénéficie de la dérogation à l'obligation d'information** prévue à l'article 14 § 5 d) du RGPD puisqu'il est soumis au secret professionnel. Il appartient en conséquent à l'entité contrôlée d'informer les personnes concernées que leurs données personnelles peuvent être transmises à leur commissaire aux comptes (**2**).

Dans les autres cas, cette information doit être fournie par le commissaire aux comptes à ses clients dans sa lettre de missions et ses supports de communication (site web, newsletter…) (**3**)

Transparence

Sommaire

L'article 5 § 1 du RGPD dispose que *« les données à caractère personnel doivent être traitées de manière licite, loyale* ***et transparente*** *au regard de la personne concernée »*.

Si le principe de transparence n'est pas en soi défini par le RGPD, le considérant 39 du règlement permet d'en comprendre la teneur :

« Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées ***devraient être transparents à l'égard des personnes physiques concernées.*** *»*

L'exigence de transparence signifie donc que les personnes concernées doivent être informées du traitement de leurs données, des modalités de ce traitement et des droits dont elles disposent[65]. Tout comme l'*accountability*, la transparence du traitement constitue un gage de confiance pour les personnes concernées (Cf. Fiche 1 du guide CNCC *« Gouvernance et accountability »*).

L'obligation d'information des personnes concernées est encadrée tant dans son contenu que dans sa forme (**1**). Bien qu'en vertu du secret professionnel le commissaire aux comptes puisse bénéficier d'une dérogation à l'obligation d'information (**2**), il est néanmoins essentiel de documenter et encadrer le respect de cette obligation (**3**).

1. Principe de transparence et obligation d'information

1.1 Le contenu de l'information

Le contenu de l'obligation d'information varie légèrement selon que les données personnelles sont collectées directement (article 13 du RGPD) ou indirectement (article 14 du RGPD) auprès de la personne concernée.

– *Qui sont les « personnes concernées » ?*

Les « personnes concernées » sont **toutes personnes physiques dont les données personnelles font l'objet d'un traitement.**

Dans le cadre des traitements mis en œuvre par le commissaire aux comptes, il s'agit notamment des salariés et contacts au sein de l'entité contrôlée, des fournisseurs, clients, prestataires, mandataires et actionnaires de celle-ci, des personnes membres des organes de contrôle de l'entité contrôlée, des collaborateurs du commissaire aux comptes, etc.

Une lecture combinée des articles 13 et 14 du RGPD permet de lister les informations qui doivent être portées à la connaissance des personnes concernées.

Dans tous les cas, l'information doit contenir :

– L'identité et les coordonnées du **responsable du traitement**.

– Les **coordonnées du délégué à la protection des données** le cas échéant.

[65] Lignes directrices du CEPD du 29 novembre 2017 sur la transparence au sens du RGPD : *« Le principe de transparence, lorsqu'il est respecté par les responsables du traitement permet aux personnes concernées de contrôler leurs données à caractère personnel et d'exiger des responsables du traitement et des sous-traitants qu'ils rendent des comptes à cet égard, par exemple en accordant ou en retirant le consentement éclairé et en faisant appliquer leurs droits en tant que personne concernée ».*

À noter : si votre cabinet ne dispose pas de DPO, il est recommandé de créer une adresse mail dédiée aux demandes d'exercice de droits que des personnes concernées pourraient vous adresser.

- Les **finalités** du traitement (en cohérence avec votre registre des traitements).

Par exemple : dans le cadre d'une mission de contrôle légal, le traitement mis en œuvre par le commissaire aux comptes a essentiellement pour finalité la certification des comptes.

- La **base juridique** du traitement (en cohérence avec votre registre des traitements).

Par exemple : le traitement de données personnelles mis en œuvre dans le cadre des missions du commissaire aux comptes a pour base légale le respect d'une obligation légale à laquelle le commissaire aux comptes est soumis.

- Les **destinataires** ou catégories de destinataires des données personnelles (identifiés dans le registre).

Par exemple : les données traitées par le commissaire aux comptes peuvent être partagées avec des actuaires, des experts et collaborateurs externes qui assistent le commissaire aux comptes dans sa mission.

- La **durée de conservation** des données personnelles (ou du moins les critères utilisés pour déterminer cette durée, tels que définis dans le registre).
- **Les droits** dont dispose la personne concernée, à savoir les **droits d'accès**[66], de **rectification**[67], d'**effacement**[68] des données, le droit à la **limitation du traitement**[69], le droit à la **portabilité**[70] de ses données, le droit d'**opposition**[71] à un traitement (sous certaines conditions), y compris celui d'introduire une réclamation auprès de la CNIL.

À noter : L'existence de certains droits varie selon la base juridique du traitement. À titre d'exemple, le droit à la portabilité ne peut être invoqué que si le traitement est fondé sur la base du consentement ou l'exécution d'un contrat auquel la personne concernée est partie. Ce droit ne s'applique donc pas aux traitements mis en œuvre par le commissaire aux comptes dans le cadre de ses missions. Il est également possible, sous certaines conditions, de faire échec à l'exercice du droit d'accès, rectification, limitation du traitement ou d'effacement de données. (Cf. Fiche n° 5 du Guide *« la gestion des droits par les personnes concernées »*[72])

[66] Le droit pour la personne concernée d'obtenir du responsable du traitement la confirmation que des données personnelles la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès à ces données ainsi que les informations énumérées à l'article 15 du RGPD.
[67] Le droit pour la personne concernée d'obtenir du responsable du traitement la rectification des données personnelles la concernant qui sont inexactes (article 16 du RGPD).
[68] Le droit d'obtenir du responsable du traitement l'effacement de données la concernant en présence l'un des motifs listés à l'article 17 du RGPD.
[69] Le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments énumérés à l'article 18 du RGPD s'applique.
[70] Le droit pour la personne concernée de recevoir les données personnelles la concernant dans un format structuré, couramment utilisé et lisible, de les transmettre à un autre responsable du traitement, ou d'obtenir que ces données soient transmises directement à un autre responsable du traitement (article 20 du RGPD).
[71] Le droit de s'opposer au traitement de ses données personnelles à des fins de prospection (article 21 du RGPD).
[72] Vous pouvez également consulter les fiches CNIL *« Respecter les droits des personnes »*, *« Les droits pour maîtriser vos données personnelles »* ou encore *« Préparer l'exercice des droits des personnes »*

– Le cas échéant, **l'existence d'un transfert de données vers des pays tiers** ou à une organisation internationale bénéficiant[73] ou non d'une décision d'adéquation.

Par exemple : si votre cabinet de commissariat aux comptes appartient à un réseau international de cabinets amené à partager des données personnelles de clients, ces derniers doivent être informés des transferts et des mesures appropriées qui ont été mises en œuvre (Cf. Fiche n° 7 *« Transferts hors UE »* du Guide).

– Le cas échéant, l'information sur la question de savoir si l'exigence de communication de données personnelles a un **caractère règlementaire ou contractuel** ou si elle conditionne la conclusion d'un contrat, le caractère facultatif ou obligatoire de la communication des données, ainsi que sur les conséquences éventuelles de la non-fourniture de données « obligatoires ».

– Le cas échéant, **l'existence d'une prise de décision automatisée** y compris un profilage, les informations utiles concernant **la logique sous-jacente** ainsi que l'importance et les conséquences de ce traitement pour la personne concernée.

– Lorsque le responsable du traitement a l'intention d'effectuer ultérieurement un traitement pour une finalité autre que la finalité initiale, il fournit à la personne concernée des informations au sujet de cette autre finalité.

En cas de collecte indirecte, l'information doit également contenir :

– La **source** d'où proviennent les données.

Par exemple : la source des données personnelles traitées par le commissaire aux comptes lors de ses missions est généralement l'entité contrôlée car c'est elle qui lui fournit les informations sur ses actionnaires, salariés, mandataires, etc.

– Les **catégories de données collectées** indirectement (Cf. Modèle de registre des traitements fourni en annexe de la Fiche 1 *« Gouvernance et accountability »* du guide CNCC).

1.2 Les modalités de fourniture des informations

L'information fournie aux personnes concernées doit être « ***concise, transparente, compréhensible*** *et* ***aisément accessible*** *en des termes clairs et simples* »[74].

La CNIL invite également les responsables du traitement à faire preuve d'efficacité en rédigeant une information la plus claire possible et en la présentant de manière succincte (Cf. Fiche de la CNIL *« Conformité au RGPD : Comment informer les personnes et assurer la transparence »*). Dans le cadre des missions de commissariat aux comptes, la lettre de mission et/ou les conditions d'intervention prévoient que l'obligation d'information repose sur l'entité contrôlée (Cf. Modèle de lettre de la CNCC, point 0).

[73] La liste des pays et territoires tiers bénéficiant d'une décision d'adéquation figure sur le site internet de la Commission européenne et de la CNIL. À ce jour, ces pays sont l'Andorre, l'Argentine, le Canada, les Îles Féroé, Guernesey, Israël, l'Île de Man, le Japon, Jersey, la Nouvelle Zélande, la Suisse, l'Uruguay.

[74] **Article 12 du RGPD** *« Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ».*

1.2.1 Concision

L'exigence de concision signifie que l'information doit être présentée de manière succincte *« afin d'éviter de noyer d'informations les personnes concernées »*[75]. L'information peut néanmoins être présentée de manière concise avec un renvoi vers un document plus détaillé (Cf. point 3.2).

1.2.2 Clarté

L'exigence de clarté signifie que l'information doit être compréhensible par la majorité du public visé.

Par exemple : dans sa lettre de mission ou dans ses conditions d'intervention, le commissaire aux comptes s'adresse à des professionnels. Il peut donc s'attendre à ce que ces personnes aient un bon niveau de compréhension concernant la protection des données.

1.2.3 Accessibilité

Les personnes concernées doivent pouvoir trouver rapidement cette information et la consulter librement, quel qu'en soit le support. Il est recommandé de mettre ces informations à disposition des personnes concernées dans un même document (généralement dans une « Politique de protection des données » ou « Charte de confidentialité », cf. point 3.2 ci-après) accessible en pied de page d'un site internet[76].

Quand l'information doit-elle être donnée aux personnes concernées ?

– **En cas de collecte directe**, l'information doit se faire au moment de la collecte des données.

Par exemple : si le site de votre cabinet comporte un onglet « recrutement » permettant à des candidats de soumettre au cabinet leur candidature à un poste ou un stage, il convient de placer une mention d'information sous le formulaire de contact afin que le candidat soit informé des modalités du traitement des données personnelles fournies dans le cadre de sa candidature.

– **En cas de collecte indirecte**, l'information doit se faire dès que possible (lors du premier contact avec la personne concernée) ou au plus tard dans le délai d'un mois[77].

Il existe cependant des dérogations à ce principe, dont une en particulier intéresse le commissaire aux comptes (**2**).

[75] **Lignes directrices du CEPD du 29 novembre 2017 sur la transparence au sens du RGPD :** *« Les responsables du traitement devraient présenter les informations/communications de façon efficace et succincte afin d'éviter de noyer d'informations les personnes concernées ».*

[76] **Ligne directrice du CEPD du 29 novembre 2017 sur la transparence au sens du RGPD :** « *Le G2 recommande que l'intégralité des informations adressées aux personnes concernées soit également consultable à un endroit unique ou dans un même document ».*

[77] Article 14 § 3 du RGPD : *« Le responsable du traitement fournit les informations visées aux paragraphes 1 et 2 :*
a) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;
b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne concernée ; ou
c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois ».

2. La dérogation à l'obligation d'information : le secret professionnel

L'article 14 § 5 du RGPD prévoit plusieurs exceptions qui sont susceptibles de dispenser le commissaire aux comptes (responsable de traitement) d'informer certaines personnes concernées.

Le commissaire aux comptes est fondé à se prévaloir de l'exception prévue à l'article 14 § 5 d) du RGPD. Aux termes de cet article, le responsable du traitement est exempté de son obligation d'informer les personnes concernées lorsque les données personnelles doivent rester confidentielles en **vertu d'une obligation de secret professionnel**[78].

Les commissaires aux comptes sont expressément soumis par la loi au secret professionnel[79] et peuvent donc bénéficier de cette dérogation. Ils n'ont pas à informer les salariés, actionnaires, et clients de l'entité contrôlée des traitements réalisés dans le cadre de leurs missions.

Par exemple : dans le cadre d'une mission de contrôle des comptes d'une entreprise, vous êtes amené à consulter divers documents confidentiels (tels que des rapports, déclarations, procès-verbaux d'assemblée générale, etc.) qui peuvent contenir des données personnelles. Ces documents sont couverts par le secret professionnel de sorte que le commissaire aux comptes n'est pas tenu d'informer les personnes dont des données personnelles peuvent figurer sur ces documents.

3. La mise en œuvre de l'obligation d'information par les cabinets de commissariat aux comptes

Si vous bénéficiez de cette dérogation dans le cadre de vos missions, il est néanmoins essentiel d'encadrer l'obligation d'information dans la lettre de mission/vos conditions d'intervention signée(s) avec l'entité contrôlée (**3.1**) et de disposer d'une politique de confidentialité et de mentions d'information (**3.2**).

3.1 La lettre de mission/vos conditions d'intervention

Le modèle de lettre de mission de la CNCC prévoit une mention d'information générale qui pourra être complétée par une mention plus détaillée.

[78] **Article 14 § 5 d) :** *« Les paragraphes 1 à 4 ne s'appliquent pas lorsque et dans la mesure où d) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel règlementée par le droit de l'Union ou le droit des États-membres, y compris une obligation légale de secret professionnel ».*

[79] **Article L. 822-15 du Code de commerce :** *« Sous réserve des dispositions de l'article L. 823-12 et des dispositions législatives particulières, les commissaires aux comptes ainsi que leurs collaborateurs et experts, sont astreints au secret professionnel pour les faits, actes et renseignements dont ils ont pu avoir connaissance à raison de leurs fonctions ».*

• **Les bonnes pratiques :**

✓ Vérifier que votre modèle type de lettre de mission/vos conditions d'intervention comportent un article relatif aux traitements des données personnelles (indiquant notamment que vous agissez en tant que responsable du traitement).

✓ Rappeler à l'entité contrôlée son obligation d'informer les personnes concernées du fait que leurs données peuvent faire l'objet d'une transmission à son/ses commissaire(s) aux comptes (destinataire).

Par exemple : le modèle de lettre de mission de la CNCC prévoit, à l'article 6.4.2 *« conformément à l'article 14 § 5 d) du RGPD,* ***nous ne sommes pas tenus d'informer les personnes concernées des traitements opérés dans le cadre de notre mission.*** *Il vous appartient donc d'informer les personnes concernées des traitements que nous réalisons »* (Cf. Modèle de lettre de mission CNCC).

3.2 Politique de confidentialité et mentions d'information

3.2.1 Politique de confidentialité

Dans ses lignes directrices sur la transparence, le CEPD invite les responsables de traitement à publier sur leur site internet une politique de confidentialité :

*« **Chaque entreprise disposant d'un site internet devrait publier une déclaration ou un avis sur la protection de la vie privée sur son site.** Un lien direct vers cette déclaration ou cet avis sur la protection de la vie privée devrait être **clairement visible sur chaque page de ce site internet** »*[80].

Cette exigence s'inscrit dans la droite ligne du respect du principe d'*accountability* auquel les commissaires aux comptes sont soumis en tant que responsable du traitement (Cf. Fiche n° 1 *« Gouvernance et accountability »* du Guide).

Pour répondre à l'exigence de transparence, votre politique de confidentialité doit permettre aux personnes concernées de connaître :

⇨ **Les modalités du traitement** de leurs données mis en œuvre par votre cabinet (mentions citées aux articles 13 et 14 du RGPD) ;

Par exemple : la politique de confidentialité peut indiquer dans la rubrique « finalités » que les traitements sont mis en œuvre aux fins de l'accomplissement par le commissaire aux comptes de ses missions légales et des prestations qui lui sont autorisées par les textes (prestations au sens du Code de déontologie, couvertes par le secret professionnel).

⇨ **Les droits** dont elles disposent sur leurs données ;

Par exemple : la personne concernée doit être informée qu'elle dispose du droit d'opposition au traitement de ses données à des fins de prospection commerciale :

« Vous disposez du droit de vous opposer à tout moment pour des raisons tenant à votre situation particulière, à l'utilisation de vos données à des fins de prospection commerciale ».

[80] Lignes directrices du CEPD du 29 novembre 2017 sur la transparence au sens du RGPD (page 9).

⇨ **La procédure à suivre/le point de contact** pour exercer ses droits ;

Par exemple : il est recommandé d'indiquer aux personnes concernées un contact (comme une adresse mail dédiée qui redirige vers la/les personne(s) en charge de la protection des données) à qui adresser leurs demandes d'exercice de droits.

• **Les bonnes pratiques :**

✓ Maintenir sur le site internet de votre cabinet une politique de confidentialité complète et accessible depuis toutes les pages du site.

✓ Veiller à ce que la rédaction de votre politique de confidentialité réponde aux exigences de clarté et de concision requises par la CNIL (Cf. point 1.2).

✓ Indiquer dans votre politique de confidentialité une adresse email/postale dédiée aux demandes d'exercice de droits.

À noter : la politique de confidentialité fait partie de la documentation *« data privacy »* qui doit être régulièrement revue, et si nécessaire mise à jour, par la personne ou le comité au sein de votre cabinet en charge des problématiques de protection des données personnelles (Cf. Fiche 1 du guide CNCC *« Gouvernance et accountability »*)

3.2.2 Mentions d'informations (newsletter, formulaires…)

Des mentions d'information doivent être placées sur le site internet du cabinet ainsi que sur chaque formulaire de collecte de données traitées par le commissaire aux comptes dans le cadre de ses missions.

Des exemples de mentions d'information figurent sur le site de la CNIL

Comment respecter l'exigence de concision tout en fournissant une information exhaustive au regard des articles 13 et 14 du RPGD ?

Afin de ne pas alourdir votre documentation, l'information des personnes concernées peut être fournie en deux étapes. Selon les cas, il peut être judicieux de rédiger une mention comportant uniquement les informations essentielles (telles que le nom du responsable du traitement et les finalités du traitement) et de renvoyer vers une notice d'information ou une politique de confidentialité plus complète (Cf. Fiche de la CNIL *« Conformité RGPD : comment informer les personnes et assurer la transparence ? »*).

L'obligation d'information s'applique-t-elle également en matière d'utilisation de cookies sur le site internet du cabinet ?

Oui, la collecte de données personnelles par des cookies constitue un traitement qui doit être porté à la connaissance des personnes concernées. Si votre site utilise des cookies, vous devez mettre en place un bandeau destiné à informer les visiteurs du dépôt de cookies sur leur équipement terminal et, en cas de cookies soumis au consentement, collecter leur consentement.

Par exemple : Ce bandeau peut être rédigé de la sorte : « ***[Nom du cabinet]****, utilise des cookies* ***[type de cookies]*** *aux fins de* ***[à adapter selon le type de cookies]*** *: J'accepte/Je refuse/Paramétrer les cookies* ***[lien vers le module cookies]****. Vous disposez du droit de retirer votre consentement à tout moment. Pour en savoir plus, consultez notre Politique de confidentialité ».*

Pour plus d'informations sur les cookies, vous pouvez vous référer aux Lignes directrices de la CNIL relatives aux opération de lecture ou écriture dans le terminal d'un utilisateur[81], à la Fiche de la CNIL *« Cookies et traceurs : que dit la loi »* ainsi qu'à la Recommandation de la CNIL sur les modalités pratiques de recueil du consentement en matière de cookies.

• Les bonnes pratiques

✓ Vérifier que vos formulaires de collecte, quel que soit leur support, disposent de mentions d'information claires et qui renvoient, si besoin, à la politique de confidentialité du cabinet.

✓ S'assurer que l'utilisation de cookies est faite de manière conforme aux recommandations de la CNIL (bandeau d'information, collecte du consentement, conservation limitée, etc.).

À noter : il est recommandé de se doter d'une politique cookies (qui peut être incluse ou non dans la politique de confidentialité) afin de permettre aux internautes visitant votre site internet de connaître les conditions dans lesquelles les cookies sont utilisés et les paramètres à régler pour les éviter.

Transparence

[81] https://www.cnil.fr/sites/default/files/atoms/files/ligne-directrice-cookies-et-autres-traceurs.pdf (2020)

Gestion des droits RGPD

Gestion des droits RGPD

Fiche n° 5

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

L'objectif de cette fiche est de vous guider dans la mise en œuvre de vos processus internes visant à répondre aux demandes d'exercice de droits dévolus par le RGPD et la Loi Informatique et Libertés formulées par les personnes concernées.

Un cabinet de commissariat aux comptes est avant tout une entreprise et peut donc à ce titre être amené à répondre à des demandes d'exercice de droits sur les traitements de données personnelles qu'il effectue.

En principe, la personne concernée dispose des droits suivants au titre de la Règlementation applicable :

- Droit d'accès aux données.
- Droit de rectification des données.
- Droit à l'effacement des données.
- Droit à la portabilité des données.
- Droit à la limitation du traitement.
- Droit d'opposition au traitement.
- Droit d'introduire une réclamation auprès de la CNIL.

Toutefois, en fonction du contexte dans lequel les données personnelles sont collectées par le commissaire aux comptes, les droits des personnes concernées seront limités notamment par les obligations relatives au secret professionnel qui s'imposent au commissaire aux comptes.

En effet, le commissaire aux comptes ne peut modifier son dossier de travail, ou en révéler le contenu à d'autres personnes que celles expressément prévues par la Réglementation (régulateur, AMF, autorités judiciaires – cf. Tableau récapitulatif CNCC *« secret professionnel »*[82]). Le commissaire aux comptes ne pourra donc pas satisfaire les demandes d'exercice de droits dirigées sur des données figurant dans son dossier de travail.

Le commissaire aux comptes peut notamment être amené à collecter des données personnelles, pouvant faire l'objet de demandes d'exercice de droits par les personnes concernées, dans les contextes suivants :

- Collecte indirecte auprès des entités contrôlées pour les traitements liés au contrôle légal (sauf les données du dossier de travail soumis au secret professionnel) : les demandes seront à traiter au cas par cas.
- Collecte directe auprès de la personne concernée pour certains traitements liés au contrôle légal (sauf pour les données figurant au sein du dossier de travail soumis au secret professionnel) telles que les données de contact au sein de l'entité contrôlée.
- Collecte directe ou indirecte de données pour des traitements liés à des sollicitations professionnelles ou à la gestion des ressources humaines ou en rapport avec des traitements courants, propres à toute entreprise (gestion des fournisseurs, de la comptabilité…).

[82] https://doc.cncc.fr/docs/secret-professionnel?q=SECRET%20PROFESSIONNEL%20tableau

Dans les cas les plus courants, lorsqu'aucune limitation ne s'applique, le commissaire aux comptes doit faciliter l'exercice des droits des personnes concernées en les informant de leur existence et des modalités d'exercice de ces droits.

Par ailleurs, le commissaire aux comptes est tenu de répondre aux droits des personnes concernées dans les temps impartis par la Règlementation applicable, soit **un mois à compter de la demande**, délai pouvant être prolongé de deux mois supplémentaires en cas de complexité ou de multiplication des demandes.

Pour répondre de manière effective à ces droits, le commissaire aux comptes devra mettre en place **des procédures internes** permettant de remonter l'ensemble des demandes au contact compétent et de suivre leur traitement afin (i) de démontrer que les délais de réponse ont été respectés, mais également (ii) de justifier des motivations d'un éventuel refus à l'exercice de certains droits (limitation des droits d'accès, demandes abusives…).

Les demandes d'exercice de droits ne peuvent cependant pas conduire à la communication de toutes les informations détenues par le commissaire aux comptes sur la personne concernée, au risque pour le commissaire aux comptes de manquer à son obligation de préservation du secret professionnel et du secret des affaires. À cet égard, **le commissaire aux comptes n'est tenu de communiquer que les seules données personnelles faisant l'objet de la demande d'exercice de droit, indépendamment du support qui les contient et de son contenu de fond.** Par conséquent, les rapports, consultations juridiques ou financières qui contiennent des données personnelles n'ont pas à être communiqués dans le cadre de l'exercice d'un droit d'accès[83].

[83] La Cour de Justice de l'Union Européenne (**« CJUE »**) a également jugé que les informations issues d'une analyse juridique ne figurent pas dans les données communiquées à l'intéressé lors d'une demande d'accès, et ce y compris lorsqu'une telle analyse juridique concerne l'intéressé et se fonde sur des *caractère personnel, elle ne constitue pas pour autant en elle-même une telle donnée* ».
La Cour rappelle également que *« c'est afin de pouvoir effectuer les vérifications nécessaires que la personne concernée dispose d'un droit d'accès aux données la concernant qui font l'objet d'un traitement »* et ainsi de pouvoir exercer les droits en résultant (rectification, effacement, suppression de ces données).
Or, une consultation juridique n'est pas *« en elle-même susceptible de faire l'objet d'une vérification de son exactitude par ce demandeur et d'une rectification »* et n'est donc pas une donnée à caractère personnel susceptible d'être communiquée lors d'une demande effectuée au titre du droit d'accès.
La CJUE conclu que *« dans la mesure où l'objectif poursuivi par ce droit d'accès peut être pleinement satisfait par une autre forme de communication, la personne concernée* ***ne saurait tenir*** [des dispositions relatives au droit d'accès au sein de la Règlementation applicable] ***le droit d'obtenir une copie du document ou du fichier original dans lequel ces données figurent.*** *(…) Par conséquent, le droit d'accès dont* [le] *demandeur peut se prévaloir* (…) *porte* ***uniquement*** *sur* [ses données à caractère personnel] ». (CJUE, 17 juill. 2014, aff. Jtes C-141/12 et C-372/12, YS c/ Minister voor Immigartie, Integratie en Asiel et Minister voor Immigratie, Integratie en Asiel c/ M.S., points 39, 44, 45, 48 et 59)

Sommaire

1. Remarques liminaires – la limitation des droits des personnes concernées à l'égard des données contenues dans le « dossier de travail » du commissaire aux comptes

Le RGPD prévoit que des limitations au droit d'accès, ainsi qu'au droit à l'information, au droit de rectification ou d'effacement, au droit à la portabilité, ou encore au droit d'opposition « *peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir (…) la prévention (…) de manquements à la déontologie des professions réglementées (…)* ».

La principale limitation applicable à l'activité du commissaire aux comptes est le secret professionnel, et ses obligations légales au titre de ses missions légales, mais également le secret des affaires. D'autres limitations propres à chaque droit seront détaillées au paragraphe 3 de la présente fiche.

⇨ Le secret professionnel du commissaire aux comptes

Le RGPD autorise une limitation des informations à fournir à la personne concernée lorsque *« les données à caractère personnel **doivent rester confidentielles** en vertu d'une obligation de secret professionnel règlementé par le droit de l'Union ou des États Membre, y compris une obligation légale de secret professionnel ».*

Les commissaires aux comptes, leurs collaborateurs et experts sont astreints au secret professionnel pour les faits, actes et renseignements dont ils ont pu avoir connaissance à raison de leurs fonctions.

La communication de documents contenant les données personnelles ne saurait avoir pour conséquence d'entraîner une violation de ces règles, lesquelles sont pénalement sanctionnées (sauf lorsque les textes délient le commissaire aux comptes au titre de son obligation à l'égard de la personne concernée).

Ainsi, le commissaire aux comptes est tenu de maintenir confidentiels certaines données ou certains documents en vertu d'une obligation de secret professionnel, cette obligation de confidentialité devra être invoquée en réponse à toute demande d'exercice de droits **pour refuser la communication des informations ou la rectification d'informations qui ont vocation à rester figées** compte tenu des obligations du commissaire aux comptes notamment en matière d'archivage et de conservation au titre de ses missions.

À noter : le commissaire aux comptes a l'obligation de conserver certaines données, même lorsqu'elles deviennent obsolètes, lors de l'accomplissement de sa mission afin de pouvoir justifier les diligences mises en œuvre. En pratique ce sera au client de mettre à jour les documents ou informations transmises au commissaire aux comptes.

Par ailleurs, en fin de mission, le dossier de travail doit être figé 60 jours après la signature du rapport[84], impliquant pour le commissaire aux comptes l'impossibilité d'y apporter des rectifications.

[84] Article R. 823-10 du Code de commerce

De même, si le commissaire aux comptes est tenu à l'égard de l'entité contrôlée par une obligation de confidentialité contractuelle supplémentaire et spécifique, le non-respect d'une telle obligation est susceptible d'engager sa responsabilité contractuelle, en complément de sa responsabilité pénale et disciplinaire.

Enfin, la violation du secret professionnel peut être caractérisée par la divulgation d'une information couverte par le secret des affaires, comme exposé ci-après.

⇨ Le secret des affaires

Le RGPD prévoit que l'exercice des droits *« ne devrait pas porter atteinte* ***aux droits ou libertés d'autrui****, y compris au* ***secret des affaires*** *ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel »*[85].

La CNIL considère également que l'exercice des droits ***« ne peut porter atteinte au secret des affaires ou à la propriété intellectuelle »***[86].

Par ailleurs, l'article L. 151-1 du Code de commerce, issu de la loi n° 2018-670 du 30 juillet 2018, dispose que :

« Est protégée au titre du secret des affaires ***toute information répondant aux critères suivants :***

1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité.

2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret.

3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret. »

Cette définition des documents couverts par le secret des affaires est extrêmement large et peut s'appliquer aux documents dont le commissaire aux comptes peut être le rédacteur ou le destinataire, puisqu'il a accès à de nombreuses informations financières et stratégiques d'une valeur commerciale évidente.

Le Code de commerce prévoit désormais des sanctions en cas d'obtention, d'utilisation ou de divulgation illicites de secrets, et notamment, en cas de production ou d'exportation en violation d'une obligation de ne pas divulguer[87].

[85] Considérant 63 du RGPD.

[86] CNIL, *« Professionnels : comment répondre à une demande de droit d'accès ? »*, du 8 août 2018, https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces, et
Le droit d'accès : connaitre les données qu'un organisme détient sur vous,
https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous

[87] Article L. 151-5 al. 1 du Code de commerce : *« L'utilisation ou la divulgation d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime par une personne qui a obtenu le secret dans les conditions mentionnées à l'article L. 151-4 ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation ».*
En cas de violation, le juge pourra allouer des dommages-intérêts en prenant en considération :
« 1° Les conséquences économiques négatives de l'atteinte au secret des affaires, dont le manque à gagner et la perte subie par la partie lésée, y compris la perte de chance.
2° Le préjudice moral causé à la partie lésée.
3° Les bénéfices réalisés par l'auteur de l'atteinte au secret des affaires, y compris les économies d'investissements intellectuels, matériels et promotionnels que celui-ci a retirées de l'atteinte ».

En conséquence, le secret des affaires pourra largement être invoqué pour motiver un refus de faire droit à une demande d'accès d'une personne concernée par le commissaire aux comptes, au même titre que le secret professionnel[88].

Dans la mesure où le dossier de travail est soumis au secret professionnel, le commissaire aux comptes n'aura pas à faire droit aux demandes concernant des données contenues au sein des dossiers de travail qu'il établit.

***

Les éléments concernant l'exercice des droits détaillés ci-après **ne sont pas applicables aux demandes visant les données personnelles** contenues au sein du « dossier de travail » établi par le commissaire aux comptes et couvert par le secret professionnel.

Nous traiterons dans cette fiche l'exercice des droits des personnes concernées dans le cadre des traitements courants réalisés par le commissaire aux comptes. À cet égard, le droit à la portabilité des données ne sera pas abordé, puisqu'il n'a pas vocation à s'appliquer compte tenu de l'activité du commissaire aux comptes.

La présente fiche aborde, dans un premier temps, les principes généraux applicables à tous les droits (information des personnes concernées, modalités d'exercice des droits et modalités de réponse) (**1**) avant de préciser les modalités spécifiques applicables à chaque droit (**2**) et leurs applications pratiques, au travers de quelques exemples (**3**).

2. Principes généraux relatifs à l'exercice des droits des personnes concernées

Conformément aux articles 15, 16, 17, 18, 20 et 21 du RGPD[89], les personnes concernées bénéficient des droits suivants :

- Droit d'accès aux données.
- Droit de rectification des données.
- Droit à l'effacement des données.
- Droit à la portabilité des données.
- Droit à la limitation du traitement.
- Droit d'opposition au traitement.
- Droit d'introduire une réclamation auprès de la CNIL.

Le commissaire aux comptes, en qualité de responsable de traitement (Cf. Fiche n° 2 du guide *« Le Statut du commissaire aux comptes »*), doit s'assurer que les personnes concernées ont été informées de l'existence et des modalités d'exercice de leurs droits (Cf. Fiche n° 4 du

[88] Par ailleurs, une violation du secret professionnel peut être caractérisée par la divulgation d'une information couverte par le secret des affaires.

[89] Articles 48, 49, 50, 51, 53, 54, 55 et 56 de la loi n° 78-17 du 6 janvier 1978 dans sa dernière version en vigueur à la date de la publication de la présente fiche (Loi Informatique et Libertés, dite « **LIL** »).

guide *« Transparence – Information »*) et *« **facilite[r] l'exercice des droits conférés à la personne concernée** au titre des articles* [suscités] »[90].

Dans le cadre des traitements mis en œuvre par le commissaire aux comptes dans le cadre de sa mission, les personnes concernées sont principalement des salariés et contacts au sein de l'entité contrôlée, des fournisseurs, clients, prestataires, mandataires et actionnaires de celle-ci, des personnes membres des organes de contrôles de l'entité contrôlée, des collaborateurs du commissaire aux comptes et de son confrère, etc.

2.1 Information des personnes concernées sur l'existence de leurs droits

Au titre du principe de transparence, le commissaire aux comptes doit respecter son obligation d'information en informant la personne concernée des droits dont elle dispose et les modalités d'exercice de ces droits.

En cas de collecte directe auprès de la personne concernée, la CNIL recommande que *« la dénomination et l'adresse du service chargé du droit d'accès doit être porté à la connaissance de la personne concernée [au moment de la collecte des données] (…) »*[91].

> *À noter :* Pour rappel, en cas de collecte de données indirecte (i.e. par l'intermédiaire de l'entité contrôlée), l'information doit être fournie au moment de la collecte (i.e. le plus souvent par l'entité contrôlée), ou au plus tard au moment de la première communication avec la personne concernée. Pour en savoir plus, vous pouvez consulter la Fiche n° 4 du guide *« Transparence – Information »* et la Fiche CNIL *« Préparer l'exercice des droits des personnes »*

2.2 Comment permettre l'exercice des droits ?

Le responsable de traitement doit préparer l'exercice des droits des personnes concernées en déterminant le destinataire des demandes et les outils et procédures permettant l'exercice effectif de ces droits dans les délais impartis.

2.2.1 Le destinataire de la demande – mise en place d'un point d'entrée centralisé

• Les principes

La CNIL recommande de mettre en place un **contact spécifiquement désigné** pour répondre aux demandes d'exercice de droits. En effet, la CNIL a eu l'occasion de se prononcer sur la question du destinataire d'une demande de droit d'accès, estimant qu'une telle *« demande doit alors **être adressée directement à la personne ou au service désigné** par le responsable du traitement pour répondre aux demandes d'accès »*[92].

À défaut de personne ou de service dédié spécifique, la CNIL considère que la personne concernée a toujours la possibilité d'effectuer sa demande *« au siège de l'organisme concerné ou à l'un de ses établissements ou représentants, **à charge pour ceux-ci d'acheminer la***

[90] Article 12, § 2° du RGPD.
[91] CNIL, Délibération n° 80-10 du 01 avril 1980, point 3.
[92] CNIL, Délibération n° 80-10 du 01 avril 1980, point 3.

demande vers la personne ou le service compétent. *Des instructions d'organisation interne devront être données en ce sens par le responsable des institutions ou entreprises publiques ou privées »*[93].

• Les bonnes pratiques

Le cabinet aura tout intérêt à mettre en place :

✓ **un point d'entrée centralisé** pour l'exercice des droits par les personnes concernées en interne. Cette solution est à privilégier.

Par exemple : le DPO ou une plateforme en ligne d'exercice des droits.

✓ OU *a minima* **un parcours interne efficace**, ce qui implique l'élaboration de procédures internes permettant de remonter les demandes au bon interlocuteur, et de les traiter dans les délais impartis et d'assurer le suivi interne de ces demandes, et

✓ **des modalités de réponse** auprès des personnes concernées qui soient compréhensibles, accessibles et formulées en des termes clairs et simples (voir les point 2.3 de la présente fiche et son Annexe).

2.2.2 Les outils permettant l'exercice effectif des droits

• Les principes

Le responsable du traitement peut fixer librement les modalités d'exercice des droits par les personnes concernées, dès lors qu'elles s'avèrent adaptées à la manière dont il interagit avec la personne concernée et qu'elles ne constituent pas un frein manifeste à l'exercice de ces droits.

En effet, le CEPD précise que :

« La modalité fournie par un responsable du traitement pour que la personne concernée puisse exercer ses droits devrait ***être adaptée au contexte et à la nature de la relation et des interactions entre le responsable du traitement et la personne concernée****. À cette fin, un responsable du traitement peut souhaiter fournir à une personne concernée* ***une ou plusieurs modalités différentes*** *pour l'exercice des droits de celles-ci, reflétant les différentes façons selon lesquelles la personne concernée interagit avec le responsable du traitement »*[94].

La CNIL donne également d'autres exemples d'implémentations possibles propres à chaque droit afin de guider les responsables de traitement dans la mise en place d'outils facilitant l'exercice des droits par les personnes concernées (voir Fiche CNIL « Préparer l'exercice des droits des personnes, 27/01/2020).

L'exercice des droits peut être effectué de manière électronique, par écrit (envoi postal) ou sur place et peut nécessiter pour la personne concernée de justifier de son identité et/ou d'un mandat[95].

[93] *Ibid.*

[94] Lignes directrices du CEPD du 29 novembre 2017, révisées au 11 avril 2018 sur la transparence au sens du RGPD (WP260 rev.01, point 54).

[95] Articles 77 et 78 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la LIL

• Les bonnes pratiques

✓ Rappeler à l'entité contrôlée qu'il lui appartient d'informer les personnes concernées sur l'existence et les modalités d'exercice de leurs droits.

✓ S'assurer du respect par vos sous-traitants éventuels de leur obligation de collaboration[96].

Par exemple : suppression ou rectification des données selon vos instructions.

✓ Éviter les procédures trop complexes, longues, ou coûteuses (numéro surtaxé). Le RGPD indique expressément que *« aucun paiement n'est exigé (…) pour prendre toute mesure au titre [des demandes d'exercice des droits des personnes concernées] »*[97].

Par exemple : fournir l'adresse e-mail (générique de préférence) du DPO ou un lien vers une plateforme d'exercice des droits.

✓ Dans le cas où un formulaire de demande d'exercice de droit(s) est mis en place, il doit :

- Permettre l'envoi de **pièces justificatives ou complémentaires, le cas échéant**[98], telles qu'une copie d'une pièce d'identité, la preuve d'un mandat, etc.
- Contenir une rubrique permettant de préciser **quel droit est exercé** (droit d'accès, rectification, etc.) et/ ou **quelle entité ou quel commissaire aux comptes est concerné** par la demande lorsque plusieurs commissaires aux comptes mettent en commun les modalités d'exercice des droits.

En outre, le responsable du traitement doit, dans la mesure du possible, informer les personnes concernées des limitations attachées à chaque droit (voir le point 3 de la présente fiche pour plus de détails sur les limitations applicables à chaque droit).

2.3 Comment répondre aux demandes d'exercice de droits ?

Après avoir énoncé les principes communs à tous les droits, nous préciserons, pour chaque droit, les modalités d'exercice et limitations associées.

2.3.1 Les principes communs à tous les droits

• Délais de réponse[99]

Le responsable du traitement doit répondre aux demandes d'exercice de droit :

→ dans les **meilleurs délais**, et

→ en tout état de cause dans **un délai d'un mois** à compter de la réception de la demande ;

→ ce délai peut être **prorogé de deux mois**, en cas de complexité ou grand nombre de demandes, moyennant l'information de la personne concernée de la prorogation et de ses motifs ;

→ ces délais sont **suspendus** lorsque le responsable du traitement a sollicité des informations supplémentaires nécessaires pour identifier la personne concernée et ce, pendant la durée nécessaire à la fourniture de la pièce demandée[100], en cas de doute raisonnable concernant

[96] Article 28 § 3 e) du RGPD.
[97] Article 12 § 5 du RGPD.
[98] Article 79 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la LIL
[99] Article 12 § 3 du RGPD.

l'identité de cette personne. Si la personne concernée ne fournit pas le justificatif demandé, le commissaire aux comptes doit l'informer, dans un délai raisonnable et compatible avec les délais susvisés, de ce qu'il ne peut donner suite à la demande initialement formulée pour ce motif.

Dans tous les cas, **vous devrez revenir vers la personne concernée au bout d'un mois** pour l'informer de l'état de sa demande (réponse, rejet motivé, prorogation)[101].

• **Les réponses**

→ **Accuser réception de la demande**

Il est recommandé d'accuser réception des demandes reçues afin de fournir les informations relatives aux délais de réponses aux personnes concernées.

Exemple d'accusé de réception d'une demande

« Madame, Monsieur,

*Nous accusons réception de votre demande du **[JJ/MM/AA]** qui sera traitée dans les meilleurs délais et au plus tard sous 30 jours à compter de cette date. Si votre demande présente une complexité particulière ou en cas d'afflux de demandes, nous vous en informerons et ce délai pourra être prolongé de 2 mois, conformément à la Réglementation européenne en vigueur.*

[Si nous vous avons demandé une pièce d'identité ou une pièce justificative de votre demande, ces délais sont suspendus jusqu'à la fourniture de la pièce en question.]

*[La politique de confidentialité de **[Nom du responsable de traitement (commissaire aux comptes ou cabinet)]** est accessible dans la rubrique « Confidentialité » du site internet **de [Nom du commissaire aux comptes ou du Cabinet].***

[insérer l'adresse et/ou lien vers la politique de confidentialité]

<Formule de Politesse> »

→ **La demande d'informations complémentaires**

Le responsable de traitement peut demander la communication de toutes pièces complémentaires lorsque la situation l'exige[102].

Vous pourrez légitimement demander (i) des informations pour confirmer l'identité de la personne concernée, et en cas de doute, (ii) un justificatif du caractère inexact, ou périmé des données enregistrées.

[100] Article 77 al. 3 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la LIL

[101] Ce point a été rappelé par la CNIL au sein de sa Fiche *« Professionnels : comment répondre à une demande de droit d'accès »*

[102] Article 77 al. 2 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la LIL

Il est ainsi permis de demander la photocopie d'un titre d'identité[103] portant la signature du titulaire en cas de « doute raisonnable » sur l'identité du demandeur[104].

Il peut exister un « doute raisonnable » en cas de suspicion d'usurpation d'identité ou de piratage[105], ou lorsque l'adresse e-mail utilisée est non professionnelle (type gmail ou autre).

Il est recommandé de procéder à la suppression de toute copie de document d'identité (CNI, passeport, titre de séjour, etc.) une fois l'identité du demandeur confirmée. Cf. Fiche n° 3 du guide CNCC *« Gestion de la relation professionnelle (Client et Prospects) »*).

Par exemple : en cas d'exercice d'un droit effectué par voie électronique, la prudence recommande de vérifier l'identité du demandeur car le risque d'usurpation d'identité est élevé[106].

Toutefois, il n'y a pas de doute raisonnable si la demande est effectuée à partir d'un espace où la personne est authentifiée.

→ La réponse (positive)

Lorsque le responsable de traitement fait droit à une demande il fournit à la personne concernée les informations relatives aux mesures prises à la suite de sa demande d'exercice de droits[107], y compris auprès de tiers[108].

Sur les modalités de réponse voir le Modèle de réponse à une demande d'exercice de droit fourni en annexe de cette fiche.

→ Refus

Pour mémoire, vous n'êtes pas tenu de répondre favorablement à toutes les demandes d'exercice de droit.

Toutefois, si vous ne donnez pas suite à une demande **vous devrez motiver** votre décision et **informer** la personne concernée **des voies de recours** dont elle dispose pour contester cette décision (réclamation devant la CNIL, coordonnées du responsable du traitement, etc.)[109].

→ Absence de réponse

L'absence de réponse n'est pas une pratique recommandée.

Lorsque le responsable de traitement ne s'est pas prononcé dans les délais impartis, la demande est réputée rejetée[110], ce qui implique que la personne concernée pourra se prévaloir de cette absence de réponse auprès de l'autorité de contrôle en cas de réclamation[111].

[103] *Pour rappel :* la CNIL considère *« que la conservation et le traitement de copies de pièces d'identité doivent faire l'objet de mesures de sécurité renforcées, telles que, par exemple, l'intégration d'un filigrane comportant la date de collecte et l'identité du responsable de traitement ou le recours à des mécanismes de chiffrement conformes au RGS, afin de se prémunir contre les risques de mésusage de ces informations et, notamment, d'utilisation ultérieure des photographies que ces pièces comprennent »* et Projet de Référentiel CNIL, https://www.cnil.fr/sites/default/files/atoms/files/referentiel-gestion-commerciale.pdf et Délibération CNIL 2018-051 du 15 février 2018

[104] Article 12 § 6 du RGPD et Article 77 al. 2 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la LIL

[105] Fiche CNIL *« Professionnels : comment répondre à une demande de droit d'accès ? »* et Fiche CNIL *« Le droit à l'effacement : supprimer vos données en ligne »*

[106] Fiche CNIL *« Professionnels : comment répondre à une demande de droit d'accès ? »*

[107] Article 13 § 3 du RGPD.

[108] Article 19 du RGPD et article 119 de la LIL.

[109] Fiche CNIL *« Professionnels : comment répondre à une demande de droit d'accès ? »* *in fine* et article 12.4 du RGPD.

[110] Article 79 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la LIL

[111] Article 12 § 4 du RGPD.

Les bonnes pratiques à mettre en œuvre

- ✓ **Conserver la preuve de la réception et des réponses** aux demandes (par exemple : mécanisme d'horodatage et de traçabilité) afin de pouvoir justifier du respect des délais auprès de la CNIL.
- ✓ **Centraliser les demandes auprès du point de contact** mentionné au sein de la lettre de mission.
- ✓ S'assurer que vos sous-traitants se conforment aux instructions données par le commissaire aux comptes pour faire droit aux demandes.
- ✓ Procéder aux vérifications d'identité nécessaires avant de faire droit à une demande d'exercice de droits et notamment avant d'envoyer des informations au titre du droit d'accès.
- ✓ Apporter une réponse, même si celle-ci est négative, dans les délais impartis.
- ✓ Vérifier que la réponse apportée ne contrevient pas aux règles professionnelles et notamment à l'obligation de secret[112].

3. Les spécificités propres à chaque droit

3.1 Droit d'accès

3.1.1 Définition et caractéristiques

Le droit d'accès aux données permet à la personne concernée[113] de questionner le commissaire aux comptes – responsable du traitement – sur l'existence ou non d'un traitement de ses données personnelles, et d'accéder aux dites données.

Mais également d'avoir accès aux informations suivantes[114], si la personne concernée en fait la demande expresse :

→ Les finalités du traitement ainsi que sa base juridique.

→ Les catégories de données à caractère personnel concernées.

→ Les destinataires ou catégories de destinataires auxquels ses données ont été communiquées en particulier les destinataires qui sont établis dans des États n'appartenant pas à l'Union européenne ou au sein d'organisations internationales.

→ Lorsque cela est possible, la durée de conservation des données ou à défaut, les critères utilisés pour déterminer cette durée.

→ L'existence du droit de demander au responsable de traitement la rectification ou l'effacement de ses données personnelles et de demander une limitation du traitement de ses données.

[112] https://doc.cncc.fr/docs/secret-professionnel?q=SECRET%20PROFESSIONNEL%20tableau
[113] Article 105 de la LIL.
[114] Article 15 du RGPD et 49 de la LIL et Voir CNIL, Guide Droit d'accès, Edition 2016

→ Le droit d'introduire une réclamation auprès de la CNIL et ses coordonnées.

→ La communication des données personnelles en cours de traitement ainsi que toute information disponible quant à leur source[115].

Le droit d'accès permet notamment à la personne concernée l'exercice effectif de ses autres droits (tels que les droits de rectification, de limitation, d'effacement).

3.1.2 Modalités de réponse

Quelles données peuvent être communiquées ?

Certaines informations ou documents n'ont pas nécessairement à être communiqués à l'intéressé, dès lors qu'ils ne constituent pas des « données personnelles ».

Seules les données personnelles elles-mêmes, doivent être communiquées indépendamment du support qui les contient et des autres informations y figurant. Par conséquent, les rapports, consultations juridiques ou financières qui contiennent des données personnelles n'ont pas à être communiqués dans le cadre de l'exercice d'un droit d'accès[116].

Il n'est donc **pas nécessaire** d'avoir recours à des outils visant à supprimer ou occulter (« caviarder ») le contenu de tels documents en vue de leur communication à la personne concernée dans un format qui ne laisserait apparaître que les données personnelles de celui-ci.

À noter : le droit du travail permet à **l'employé de demander l'accès à son « dossier professionnel »** et donc à davantage d'informations que le droit d'accès « classique » au titre de la Règlementation applicable, telles que : des données relatives à son recrutement, son historique de carrière, l'évaluation de ses compétences professionnelles, etc.[117].

Comment la réponse doit-elle être formulée ?

Afin que le responsable de traitement puisse satisfaire une demande d'exercice de droit d'accès *« il suffit que* [le] *demandeur soit mis en possession d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme permettant à ce demandeur de prendre*

[115] Article 105 de la LIL.

[116] La Cour de Justice de l'Union Européenne (« **CJUE** ») a également jugé que les informations issues d'une analyse juridique ne figurent pas dans les données communiquées à l'intéressé lors d'une demande d'accès, et ce y compris lorsqu'une telle analyse juridique concerne l'intéressé et se fonde sur des données le concernant, dès lors que si une analyse juridique *« peut certes contenir des données à caractère personnel, elle ne constitue pas pour autant en elle-même une telle donnée »*.
La Cour rappelle également que *« c'est afin de pouvoir effectuer les vérifications nécessaires que la personne concernée dispose d'un droit d'accès aux données la concernant qui font l'objet d'un traitement »* et ainsi de pouvoir exercer les droits en résultant (rectification, effacement, suppression de ces données).
Or, une consultation juridique n'est pas *« en elle-même susceptible de faire l'objet d'une vérification de son exactitude par ce demandeur et d'une rectification »* et n'est donc pas une donnée à caractère personnel susceptible d'être communiquée lors d'une demande effectuée au titre du droit d'accès.
La CJUE conclu que *« dans la mesure où l'objectif poursuivi par ce droit d'accès peut être pleinement satisfait par une autre forme de communication, la personne concernée* ***ne saurait tenir*** [des dispositions relatives au droit d'accès au sein de la Règlementation applicable] ***le droit d'obtenir une copie du document ou du fichier original dans lequel ces données figurent.*** (…) *Par conséquent, le droit d'accès dont [le] demandeur peut se prévaloir* (…) *porte* ***uniquement*** *sur* [ses données à caractère personnel] ». (CJUE, 17 juill. 2014, aff. Jtes C-141/12 et C-372/12, YS c/ Minister voor Immigartie, Integratie en Asiel et Minister voor Immigratie, Integratie en Asiel c/ M.S., points 39, 44, 45, 48 et 59)

[117] Pour plus de détails sur les informations pouvant être demandées par un employé à son employeur : CNIL, Fiche *« L'accès à son dossier professionnel »* 9 mai 2019

connaissance desdites données et de vérifier que ces dernières sont exactes et traitées de manière conforme à [la Règlementation applicable *en matière de protection des données personnelles], afin qu'il puisse, le cas échéant, exercer les droits qui lui sont conférés par la dite [Réglementation] »*[118].

La communication d'un **tableau de synthèse** indiquant le type de données concernées et les documents qui y font référence (exemple : rapport d'analyse, consultation juridique, e-mails, comptes rendus de réunion…) peut répondre à cet objectif.

Un modèle de lettre de réponse et un exemple de tableau de synthèse figurent en Annexe de la présente fiche.

3.1.3 Limitations au droit d'accès

– Lorsqu'il porte atteinte au secret professionnel.

– Lorsqu'il porte atteinte au secret des affaires.

– Lorsque les demandes sont abusives, infondées, ou que les données ont été effacées.

Le responsable de traitement n'est pas tenu de répondre aux demandes si :

→ Elles sont **infondées ou excessives** notamment par leur caractère répétitif (nombreuses demandes, rapprochées dans le temps ou lorsqu'une copie a déjà été fournie), ou

→ Les données ne sont plus conservées ou ont été effacées. Dans ce cas l'accès est impossible.

Par exemple : Pas d'accès possible en cas de suppression des données après expiration du délai de conservation conformément à la loi ou une politique d'archivage, ou en cas de demande de suppression par une personne concernée antérieure à ce délai.

– Lorsqu'il porte atteinte aux droits et libertés d'autrui[119]

Le responsable de traitement pourra *« refuser ou limiter le droit d'accès de la personne concernée »*[120].

Dans le Guide publié par la CNIL relatif au droit d'accès, celle-ci précise bien que ce *« droit d'accès doit s'exercer* ***dans le respect du droit des tiers*** »[121].

Par exemple : il n'est pas possible de demander à accéder aux données concernant une autre personne concernée telle que son conjoint, ou d'un autre salarié d'une entreprise, etc.

[118] *Ibid.*
[119] *Article 15 § 4 du RGPD et Article 23 § 1 i) du RGPD.*
Et Article 107, I, 5° de la LIL : « (…) qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant compte des droits fondamentaux et des intérêts légitimes de la personne pour (…) protéger les droits et libertés d'autrui ».
[120] *Article 70-21 II. 2° de la LIL (ancien), Article 107, II, 2° de la LIL modifiée le 12 décembre 2018 (nouveau).*
[121] CNIL, *Guide Droit d'accès*, Édition 2016, http://www.cil.cnrs.fr/CIL/IMG/pdf/cnil_droit_d_acces-pdf_0_0.pdf

3.2 Droit de rectification

3.2.1 Définition et caractéristiques[122]

Ce droit permet d'obtenir du responsable du traitement **la rectification** des données personnelles qui sont inexactes et/ou incomplètes y compris en fournissant une déclaration complémentaire[123].

La personne concernée aura pu constater l'inexactitude des données soit par l'exercice de son droit d'accès, soit par tout autre moyen (consultation d'un rapport, d'un site internet, etc.).

3.2.2 Modalités de réponse

Quelles informations fournir s'agissant des droits de rectification, effacement et limitation ?

Vous devrez confirmer avoir procédé aux opérations de rectification demandées et, lorsque la personne concernée le demande, vous devrez en justifier auprès d'elle[124].

Si les données personnelles ont été transférées à un tiers, vous devrez effectuer les démarches nécessaires à leur rectification/effacement/limitation **auprès de ces derniers et justifier** de ces démarches auprès de la personne concernée[125].

En cas de contestation sur la pertinence des données, la charge de la preuve incombe au responsable du traitement auprès duquel est exercée la demande sauf lorsqu'il est établi que les données contestées ont été communiquées par la personne elle-même ou avec son accord[126].

Les pièces complémentaires propres au droit de rectification :

Vous pourrez légitimement demander un justificatif du caractère inexact, ou périmé des données enregistrées.

Par exemple : production de justificatif de domicile en cas de changement d'adresse, copies de diplômes, etc.).

Toutefois, vous devrez veiller à ne pas demander à la personne concernée des pièces justificatives qui seraient abusives ou disproportionnées par rapport à la demande de rectification sollicitée[127].

3.2.3 Limitations au droit de rectification

Le RGPD prévoit que des limitations au droit d'accès, ainsi qu'au droit à l'information, au droit de **rectification** ou d'effacement, au droit à la portabilité, ou encore au droit d'opposition, *« peuvent être imposées par le droit de l'Union ou le droit d'un État-membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir (…) la prévention*

[122] Article 16 du RGPD et 50 de la LIL.
[123] *Ibid.*
[124] Article 19 du RGPD et Article 106, II de la LIL.
[125] *Ibid.*
[126] Article 106, II de la LIL.
[127] *Le droit de rectification : corrigez vos informations*, fiche CNIL https://www.cnil.fr/fr/le-droit-de-rectification-corriger-vos-informations

*des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales (…) et la prévention (…) de **manquements à la déontologie** des professions réglementées (…) »*[128].

En pratique, le droit de rectification sera rarement limité. En effet, il s'agit d'un principe essentiel de la Règlementation applicable, à savoir de traiter des données à jour et pertinentes.

Ainsi, par exemple, le droit de rectification ne s'applique pas aux traitements littéraires, artistiques et journalistiques[129]. Cette limitation a peu d'impact concernant les traitements effectués par le commissaire aux comptes.

3.3 Droit à l'effacement des données (ou droit à l'oubli)[130]

3.3.1 Définition et caractéristiques

Ce droit permet d'obtenir du responsable du traitement **l'effacement des données personnelles** qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite en raison (i) de la disparition de la finalité, (ii) du retrait du consentement (si c'est la base légale utilisée), (iii) d'une opposition au traitement, (iv) d'un traitement illicite, (v) du respect d'une obligation légale.

Ce droit peut être mis en œuvre soit par le **verrouillage des données**, soit par la **suppression définitive des données**[131].

3.3.2 Modalités de réponse

Quelles informations fournir ?

Ces informations sont les mêmes que celles évoquées au point 3.1.2 ci-avant.

Quelles mesures mettre en œuvre ?

Dans les cas où le droit à l'effacement trouverait à s'appliquer, le responsable de traitement devra s'assurer que les données de la personne concernée sont bien effacées ou verrouillées[132] mais également qu'elles ne font plus l'objet d'aucun traitement[133].

> *À noter :* en cas de non-exécution de l'effacement des données ou en cas d'absence de réponse de la part du responsable du **traitement dans un délai d'un mois**, la personne concernée peut saisir la CNIL qui se prononce sur cette demande dans un délai de 3 semaines à compter de la date de réception de la réclamation[134].

3.3.3 Limitations au droit à l'effacement

La personne concernée ne pourra pas demander au responsable de traitement la suppression des données personnelles la concernant lorsque ce droit empêche :

[128] Considérant 73 du RGPD.
[129] Article 67 de la LIL (ancien), article 80 de la LIL modifiée le 12 décembre 2018 (nouveau).
[130] Article 17 du RGPD et 51 de la LIL.
[131] Article 119, III de la LIL.
[132] Article 119, III de la LIL.
[133] Considérant 65 du RGPD.
[134] Article 51 de la LIL.

– l'exercice du droit à la liberté d'expression et d'information ;

– le respect d'une obligation légale ;

Par exemple : obligation de conserver les dossiers de travail 6 ans (article R. 821-68 du Code de Commerce), obligation de conserver les bulletins de paie pendant 5 ans (article L. 3243-4 du Code du Travail) ou de faire figurer le nom des gérants et des administrateurs légaux dans les statuts d'une société ou de publier la liste des représentants du personnel au sein d'une entreprise) ;

– la constatation, à l'exercice ou la défense de droits en justice[135] ;

Par exemple : dans le cadre d'un précontentieux ou contentieux avec un salarié ou client.

Le commissaire aux comptes peut donc légitimement refuser de faire droit à des demandes d'effacement lorsque (i) une obligation légale lui impose la conservation des données ou (ii) la conservation des données est nécessaire à la constatation, à l'exercice ou la défense de droits en justice.

Par ailleurs, le RGPD prévoit que des limitations au droit d'accès, ainsi qu'au droit à l'information, au droit de rectification ou **d'effacement**, au droit à la portabilité, ou encore au droit d'opposition, *« peuvent être imposées par le droit de l'Union ou le droit d'un État-membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir (…) la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales (…) et la prévention (…) de* ***manquements à la déontologie*** *des professions réglementées (…) »*[136].

3.4 Droit à la limitation du traitement[137]

3.4.1 Définition et caractéristiques

Ce droit permet d'obtenir du responsable du traitement **une limitation du traitement de ses données personnelles** et s'applique uniquement dans les cas suivants :

→ L'exactitude des données est contestée.

→ Lorsque la personne concernée s'oppose au traitement pour des raisons tenant à sa situation particulière (voir ci-après « droit d'opposition »).

→ Lorsque les données sont devenues inutiles pour le responsable du traitement mais qu'elles restent nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice.

→ Lorsque la personne concernée s'oppose à l'effacement de données traitées de manière illicite et demande la limitation du traitement.

Le RGPD le définit comme *« un marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur »*[138].

[135] Article 17, 3° du RGPD.
[136] Considérant 73 du RGPD.
[137] Article 18 du RGPD.
[138] Article 4 du RGPD.

À noter : lorsque le traitement a été limité conformément aux conditions ci-avant, **les données ne peuvent être traitées** – sauf s'agissant de leur conservation – **que** (i) avec le consentement de la personne concernée, ou (ii) pour la constatation, l'exercice ou la défense de droits en justice, ou (iii) pour la protection des droits d'une autre personne physique ou morale, ou encore (iv) pour des motifs importants d'intérêt public de l'Union européenne ou d'un État membre[139].

3.4.2 Modalités de réponse

Quelles informations fournir s'agissant des droits de rectification, effacement et limitation ?

Cf. point 3.1.2 de la présente fiche.

Quelles mesures mettre en œuvre ?

Parmi les méthodes possibles de limitation du traitement par le responsable du traitement, le RGPD propose, à titre indicatif et non limitatif, de déplacer temporairement les données en cause vers un autre système de traitement, de les rendre inaccessibles aux utilisateurs, ou de retirer temporairement ces données publiées sur un site internet[140].

3.4.3 Limitations au droit à la limitation du traitement

Dès lors qu'une limitation de l'utilisation des données concernées a été demandée, le responsable du traitement ne peut utiliser les données en cause que dans les cas[141] suivants :

- la personne concernée a donné son accord ;
- pour la constatation, l'exercice ou la défense de droits en justice ;
- pour la protection des droits d'une autre personne physique ou morale ;
- pour des motifs importants d'intérêt public de l'Union européenne ou d'un État-membre.

Dès lors que la limitation en question du traitement est levée, alors qu'elle avait été accordée, le responsable du traitement doit, au préalable, en informer la personne concernée[142].

En pratique, le droit à la limitation du traitement est très rarement demandé. Toutefois, ce droit ne doit pas être utilisé pour restreindre l'exercice de votre mission ou votre obligation de conserver les dossiers de travail.

Par exemple : un Comité Social et Économique (CSE) qui viendrait refuser la communication au commissaire aux comptes de fichiers comptables et analytiques comportant des données personnelles ou contenant des données anonymisées. Cette pratique, conduisant à imposer une limitation du traitement de données personnelles peut entraver la bonne conduite de sa mission par le commissaire aux comptes.

[139] Article 18 § 2 du RGPD.
[140] Considérant 67 du RGPD.
[141] Article 18 § 2 du RGPD.
[142] Article 18 § 3 du RGPD.

À noter : bien que l'exercice de ce droit ne puisse entraver la réalisation de votre mission, en tant que responsable du traitement vous devrez apprécier au cas par cas et mettre en balance la nécessité et l'étendue de votre traitement avec les libertés individuelles des personnes concernées.

3.5 Droit d'opposition au traitement

3.5.1 Définition et caractéristiques

Ce droit permet d'obtenir du responsable de traitement qu'il cesse de traiter les données personnelles pour des raisons tenant *« à la situation particulière »* de la personne concernée.

Ce droit s'applique uniquement aux traitements fondés sur les bases légales suivantes : (i) l'intérêt légitime du responsable du traitement ; ou (ii) l'exécution d'une mission d'intérêt public.

Ce droit n'est pas un droit à la suppression simple et définitive de toutes les données de la personne concernée.

À noter : **en cas de sollicitation professionnelle**, la personne concernée peut s'opposer **à tout moment** au traitement de ses données à des fins de prospection, y compris au profilage dans la mesure où il est lié à cette prospection[143]. Outre ce cas, le responsable du traitement pourra justifier son refus de répondre à une telle demande (Cf. Fiche n° 3 du guide *« Gestion de la relation professionnelle (Client et Prospects) »*)

Nota Bene – Distinction entre droit d'opposition et droit à la limitation du traitement

Le droit à la limitation peut venir en complément du droit d'opposition si ses conditions sont remplies. Quand le droit d'opposition peut s'exercer à tout moment pour des raisons tenant à la situation particulière de la personne concernée, le droit à la limitation ne s'applique que dans un nombre limitatif de cas (Cf. point 3.4).

3.5.2 Modalités de réponse

Quelles informations fournir s'agissant du droit d'opposition ?

Ces informations sont les mêmes que celles évoquées au point 3.1.2 ci-avant.

À noter : le droit d'opposition doit être porté à la connaissance de la personne concernée ***au plus tard au moment de la première communication*** *avec celle-ci et doit être* ***présenté clairement et séparément de toute autre information***[144].

Quelles mesures mettre en œuvre ?

Le responsable de traitement **doit cesser de « traiter les données** à caractère personnel, à moins :

[143] Article 21 § 2 du RGPD.
[144] Article 21 § 4 du RGPD.

- de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement **qui prévalent** sur les intérêts et les droits et libertés de la personne concernée, **ou pour la constatation, l'exercice ou la défense de droits en justice** », et/ou
- qu'au moins l'une des limitations énoncées ci-après soient applicables.

3.5.3 Limitations au droit d'opposition

Si le traitement de données a pour base légale le consentement de la personne concernée, il suffit à la personne concernée de notifier le retrait de son consentement pour mettre un terme au traitement en question (par exemple en matière de prospection commerciale dans des rapports B to C), plutôt que de faire jouer son droit « d'opposition ».

Le responsable de traitement peut refuser de faire droit à une demande d'opposition lorsque :

- le traitement a pour base légale (i) l'exécution d'un contrat, (ii) une obligation légale, ou encore (iii) un intérêt vital[145], en démontrant l'existence de « motifs légitimes et impérieux » prévalant sur les intérêts et les droits et libertés de la personne concernée[146] ;
- Par exemple : en cas de gestion des conflits d'intérêts, de sécurité, en cas de *précontentieux ou contentieux avec un salarié, etc. ;*
- l'application de ce droit est expressément écartée par une disposition légale autorisant le traitement[147].

Le Conseil d'État estime que **toute limitation à l'exercice du droit d'opposition doit se fonder sur un motif d'intérêt général et doit avoir pour finalité d'assurer l'effectivité du traitement**[148]. Le G29 considère que *« certains intérêts peuvent être impérieux et profitables à la société en général, comme l'intérêt de la presse à publier des informations sur des faits de corruption dans l'administration (…) »*[149].

Enfin, le RGPD prévoit que des limitations au droit d'accès, ainsi qu'au droit à l'information, au droit de rectification ou d'effacement, au droit à la portabilité, ou encore **au droit d'opposition**, *« peuvent être imposées par le droit de l'Union ou le droit d'un État-membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir (…) la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales (…) et la prévention (…) de* ***manquements à la déontologie*** *des professions réglementées (…) »*[150].

[145] Article 6, points a), b), c), et d) du RGPD.
[146] Fiche CNIL relative au droit d'opposition, https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees
[147] Article 38 al. 3 de la LIL (*idem* note 47).
[148] CE, 11 avril 2014, n° 352473, Ligue des droits de l'Homme et a. : JurisData n° 2014-007172 : Le Conseil d'État a jugé comme répondant à ces exigences un système relatif à la gestion informatisée des détenus en établissement pénitentiaire dès lors qu'il entend *« d'une part, concilier l'intérêt général qui s'attache au maintien de la sécurité et du bon ordre dans les établissements pénitentiaires, à la prévention de la récidive et à la protection effective de l'intégrité physiques des personnes détenues, avec la protection de la vie privée et, d'autre part, assurer l'effectivité des finalités poursuivies par le traitement en cause ».*
[149] G29 Lignes directrices relatives à la notion d'intérêt légitime, WP 217 du 9/04/2014
[150] Considérant 73 du RGPD.

4. Applications pratiques

4.1 Un collaborateur quitte le cabinet – Demande d'accès et d'effacement des données relatives au collaborateur sortant

Un de vos collaborateurs quitte votre cabinet et demande à avoir accès à et/ou la suppression de l'ensemble des données à caractère personnel qui permettent de l'identifier directement ou indirectement (emails, feuilles de temps, signature des papiers de travail…).

Ces informations sont contenues dans vos systèmes (SI RH, CRM…) ainsi que dans les différents dossiers de travail relatifs à des entités contrôlées.

⇨ S'agissant des données contenues au sein de vos outils internes, vous pourrez vous limiter à la communication des données identifiantes (directement ou indirectement) sans avoir à communiquer les documents dans leur intégralité (Cf. point 3.1.2 « Quelles données peuvent être communiquées ? »).

⇨ S'agissant des données contenues dans vos dossiers de travail, celles-ci sont couvertes par le secret professionnel et une obligation de conservation. Il n'est donc pas possible de faire droit à cette demande d'accès ou de suppression.

À noter : la CNIL considère que *« sur simple demande et sans avoir à la motiver, **un candidat ou un employé** peut obtenir une copie des données qui le concernent (recrutement, historique de carrière, rémunération, évaluation des compétences, dossier disciplinaire…) »*[151].

4.2 Un candidat demande l'accès ou la suppression de ses données

Lorsque vous collectez des informations relatives à un candidat, le traitement a pour finalité le recrutement.

Le candidat qui n'a pas été retenu peut demander la destruction de son dossier à tout moment. En toute hypothèse, la CNIL considère que si un candidat ne demande pas la destruction de son dossier, les données y figurant doivent être automatiquement détruites 2 ans après le dernier contact de l'entreprise avec ce candidat.

Seul un accord formel du candidat permettrait une conservation plus longue.

Dès lors, vous devrez faire droit aux demandes de suppression des données relatives à des candidats.

4.3 Un salarié d'une entité contrôlée souhaite exercer ses droits auprès de votre cabinet

Ce type de demande peut survenir dans un contexte de litige entre un employé et son employeur, l'employé cherchant à obtenir auprès du commissaire aux comptes des informations ou pièces pour étayer son dossier.

[151] CNIL, « Travail et vie privée », Edition 2018. Et voir point 3.1.2 de la présente fiche.

Lorsque les informations demandées figurent au sein du dossier de travail du commissaire aux comptes, ce dernier manquerait à son secret professionnel en fournissant lesdites informations.

Par exemple, le salarié d'une entité contrôlée qui vous demande les extraits de ses données liées à la paie sur les trois dernières années dans le cadre d'un litige salarial avec son employeur. Ces documents figurent au sein du dossier de travail et sont couverts par le secret professionnel.

Vous pouvez indiquer au salarié de l'entité contrôlée qui vous contacte de s'adresser directement auprès de son employeur (responsable du traitement de ses données) pour exercer ses droits, et que vous n'êtes pas en mesure de faire droit à sa demande. Par ailleurs, le salarié dispose d'un droit d'accès plus étendu à l'égard de son employeur, auquel il peut demander davantage d'informations (évaluations, historique de carrières, etc.).

Annexe 1 – Modèle de réponse droit d'accès

Attention : ce document est un modèle à adapter selon le cas

Madame, Monsieur,

Nous revenons vers vous à la suite de votre demande de **consultation/accès/rectification, etc.** ***(<modifier/supprimer la mention inutile>)*** de vos données personnelles, en date du ***[DATE]*** nous avons effectué les recherches et diligences nécessaires conformément aux dispositions de la réglementation applicable en matière de protection des données personnelles.

[OPTION 1 : demande relative à d es données personnelles contenues dans des documents/fichiers **non couverts par le secret professionnel ou toute autre limitation** (informations figurant par exemple au sein du CRM)].

Nous vous prions de bien vouloir trouver dans ***[l'annexe/le tableau ci-joint]*** les données à caractère personnel vous concernant telles que conservées dans notre base de données.

En dehors de la consultation et du stockage des documents mentionnés [à ***l'annexe/au tableau ci-joint], nous n'avons pas effectué et n'effectuons pas d'autre traitement de vos données personnelles. (à supprimer/modifier le cas échéant).***

[OPTION 2 : demande relative à des données personnelles contenues dans des documents/fichiers **couverts par le secret professionnel** (par exemple : « dossier de travail » du commissaire aux comptes, documents relatifs à la mission)].

Le contenu de notre rapport, notre dossier de travail, y inclus les pièces qui nous ont été communiquées par notre client étant couverts par le secret professionnel conformément à l'article L 822 15 du code de commerce, nous ne sommes pas en mesure de faire droit à votre demande et vous invitons à vous rapprocher de ***[nom de l'entité contrôlée]*** *afin d'exercer vos droits.*

Pour toutes questions supplémentaires concernant l'utilisation de vos données à caractère personnel ou pour l'exercice de vos autres droits, vous pouvez toujours nou s contacter ***[préciser les coordonnées du DPO, le cas échéant, ou du contact interne data privacy]***.

Dans le cas où vous considérez cette réponse insatisfaisante, vous conservez le droit d'introduire une réclamation auprès de la CNIL : lien

[Formule de politesse]

[Signataire]

Données personnelles relatives à *[Nom de la personne concernée]* traitées par *[Nom du responsable du traitement]*

<À noter : La personne concernée a le droit d'obtenir du responsable du traitement ***la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données personnelles*** *ainsi que* ***les informations*** *figurant dans le tableau ci-dessous.*[152]

Les personnes concernées pourront demander d'avoir accès à leurs données personnelles mais vous n'avez aucune obligation de leur transmettre le document qui les contient ou d'autres informations n'entrant pas dans la définition de « données à caractère personnel » au sens de la Règlementation applicable. Il s'agira par exemple de leurs nom, prénom, date de naissance, contenus dans vos documents et/ou fichiers informatiques. Par exemple, ce droit n'impose pas pour un candidat de lui fournir l'accès aux notes prises durant l'entretien. Attention en revanche, un employé peut avoir accès à davantage d'informations auprès de son employeur (voir § 3.1.2).

Vous ne devez répondre qu'à la demande de la personne concernée et rien de plus, dans les limites évoquées ci-dessus. En conséquence, les ***colonnes du tableau ci-dessous n'ont pas vocation à être toutes complétées****, et vous n'avez à remettre* ***aucun autre document.>***

Documents concernés (et objets)* <supprimer les colonnes inutiles, les informations nécessaires *a minima* comporte un « * »>	Catégories de données personnelles y figurant* *Article 15 § 1 (b) du RGPD*	Finalités du traitement* *Article 15 § 1 (a) du RGPD*	Durée de conservation ou critères de détermination de la durée* (si demandé) *Article 15, 1 d) du RGPD*	En cas de collecte indirecte, source des données *Article 15 § 1 (g) du RGPD*	Catégories de destinataires auxquels les données ont été ou seront communiquées *Article 15 § 1 (c) du RGPD*	Existence d'une prise de décision automatisée (OUI/NON) *Article 15 § 1 (h) du RGPD*
		e.g. mission d'audit	***e.g. Durée de prescription de droit commun***			

Les documents visés ci-dessus ne constituent pas des données personnelles et sont couverts par le secret professionnel ainsi que par le secret des affaires, tels que définis par la législation française applicable. ***[Nom du responsable du traitement]*** est soumis au secret professionnel et tenu, à l'égard de ses clients, de protéger le secret de leurs affaires, sous peine de voir sa responsabilité engagée. Par conséquent, nous attirons votre attention sur le fait votre droit d'accès ne vous autorise pas à avoir accès à ces documents. Cette limite à votre droit d'accès est légitime et conforme à la réglementation applicable en matière de protection des données personnelles. Pour plus d'informations, veuillez contacter ***XX***

[152] Article 15 § 1 du RGPD.

Le RGPD dans un contexte Co-CAC

Le RGPD
dans un contexte Co-CAC

Fiche n° 6

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

La présente fiche est un *addendum* à l'ensemble du guide, elle doit être lue à la lumière des autres fiches, notamment des fiches n° 2 *(« Statut du commissaire aux comptes »)* et n° 8 *(« Sécurité des données »)*.

Dans le cadre d'une mission de co-commissariat aux comptes, les commissaires aux comptes agissent chacun en tant que responsable du traitement *indépendant* dans la mission qui leur est attribuée. Ils ne sont pas responsables conjoints du traitement car ils ne déterminent pas ensemble les moyens ni les finalités d'un traitement commun[153] **(1).**

En cas d'incident de sécurité survenant au cours de la mission de co-commissariat aux comptes, il convient de :

1. Déterminer s'il s'agit ou non d'une violation de données à caractère personnel au sens de la Règlementation applicable, c'est-à-dire d'une *« violation de sécurité entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données »*[154] **(2.1).**
2. Dans l'affirmative, il convient de déterminer qui est responsable (le client ou l'un des co-commissaires aux comptes) et convenir d'un *modus operandi* quant aux notifications à effectuer (auprès de la CNIL, de l'entité contrôlée ou des personnes concernées) **(2.2).**

[153] En effet, bien que leur approche d'audit puisse être concertée conformément à la NEP 100, les traitements sont distincts.
[154] Article 4 12) du RGPD.

Sommaire

1. Les co-commissaires aux comptes : des responsables du traitement indépendants et non conjoints

Le responsable du traitement est défini à l'article 4 du RGPD comme *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».*

Certaines entités contrôlées s'interrogent sur le statut des co-commissaires aux comptes (responsables du traitement ou responsables conjoints ?). Si la qualification de responsable de traitement indépendant ne fait pas débat, la notion de « responsabilité conjointe » peut nécessiter un éclaircissement auprès de l'entité contrôlée.

Dans le cadre d'une mission de co-commissariat, les commissaires aux comptes agissent chacun en tant que responsables indépendants des traitements de données à caractère personnel qu'ils réalisent.

Lorsque l'un des co-commissaires aux comptes met à disposition de l'entité contrôlée et de l'autre co-commissaire aux comptes un outil de partage de fichiers/de travail collaboratif, il demeure responsable de la sécurité et du bon fonctionnement de cet outil à l'égard de son confrère et de l'entité contrôlée, sous réserve de la bonne utilisation de l'outil conformément à des règles d'utilisation qu'il est prudent de faire connaitre aux autres parties prenantes.

Chaque co-commissaire aux comptes est libre de mener sa mission comme il l'entend (sous réserve d'une approche d'audit concertée conformément à la NEP 100) et de définir dans sa propre organisation, les pièces et éléments qui lui sont nécessaires pour mener à bien sa mission. De plus, chaque cabinet est responsable des mesures de sécurité mises en place. Par conséquent, les co-commissaires aux comptes ne sont pas des responsables conjoints d'un même traitement et chacun demeure seul responsable de ses actes.

2. La gestion des violations de données lors d'une mission de co-commissariat aux comptes

Il peut arriver au cours d'une mission de co-commissariat aux comptes qu'un incident de sécurité survienne concernant des données personnelles confiées par l'entité contrôlée aux commissaires aux comptes.

En pareille situation, il convient de déterminer si cet incident de sécurité constitue ou non une violation de données au sens de la Règlementation applicable **(2.1).** Dans l'affirmative, il faudra déterminer l'origine de la violation de données et déterminer qui doit agir en conséquence **(2.2).**

2.1 Déterminer s'il s'agit d'une violation de données personnelles

La violation de données à caractère personnel est définie par le RGPD comme *« une violation de sécurité entrainant de manière accidentelle ou illicite, la destruction, la perte, l'altération,*

la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données »[155]. Elle est également définie en des termes quasi-identiques par la Loi informatique et liberté[156].

La notion de violation de données à caractère personnel couvre un large panel de situations (Cf. Fiche n° 8 du guide *« Sécurité des données »*). Dans un contexte de co-commissariat aux comptes, il pourrait notamment s'agir :

– D'un acte malveillant émanant d'un tiers.

Par exemple : vol d'un ordinateur ou téléphone professionnel d'un salarié.

– D'un acte interne purement accidentel.

Par exemple : l'envoi par erreur d'un fichier client à des destinataires qui n'auraient pas dû recevoir ce fichier (divulgation non-autorisée de données), la perte d'ordinateur ou d'autre dispositif de stockage par l'un des collaborateurs (il est rappelé que le recours à des dispositifs de stockage, type clé usb non cryptée, n'est pas recommandé).

À noter : ce travail de qualification préalable est important car tout incident de sécurité ne constitue pas nécessairement une violation de données à caractère personnel[157].

2.2 Déterminer qui est à l'origine de la violation de données et les actions à mettre en place

2.2.1 Si la violation de données personnelles émane de l'entité contrôlée, la violation relève de la seule responsabilité de cette dernière et ne concerne pas les co-commissaires aux comptes. Ils n'ont pas d'action à mener auprès de la CNIL ou des personnes concernées.

2.2.2 Si la violation de données personnelles provient de l'un des co-commissaires aux comptes, l'autre co-commissaire aux comptes qui n'aurait pas commis de faute n'a pas à faire de notification à la CNIL, ni aux personnes concernées (pas de responsabilité conjointe ou solidaire). Le commissaire aux comptes qui est responsable de la violation de données doit :

– Informer l'entité contrôlée,

[155] Article 4 § 12 du RGPD.

[156] **Article 83 de la loi informatique et liberté :** *« on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement ».*

[157] **Lignes directrices du CEPD du 6 février 2018 sur les violations de données à caractère personnel :** *« Il convient avant tout de garder à l'esprit qu'une violation est une forme d'incident de sécurité. Toutefois, comme indiqué à l'article 4, paragraphe 12, le RGPD ne s'applique que lorsqu'il s'agit d'une violation de données à caractère personnel (…). Si toutes les violations de données à caractère personnel constituent des incidents de sécurité, tous les incidents de sécurité ne constituent pas nécessairement des violations de données à caractère personnel ».*

- Notifier la violation de données personnelles à la CNIL tout en se coordonnant avec l'entité contrôlée qui peut être amenée, elle aussi, à effectuer une déclaration et/ou à communiquer auprès des personnes concernées selon la nature de l'incident (Cf. Fiche n° 8 du guide *« Sécurité des données »*),
- En outre, le co-commissaire aux comptes doit apprécier s'il est opportun d'informer son co-commissaire aux comptes de cette violation (collaboration raisonnable entre les co-commissaires aux comptes pour investiguer).

2.2.3 En cas de doute sur l'origine de la violation et s'il existe un risque pour les personnes concernées, la prudence recommande que chaque commissaire aux comptes et l'entité contrôlée effectuent une notification auprès de la CNIL. Une collaboration raisonnable entre les co-commissaires aux comptes et l'entité contrôlée peut être nécessaire afin d'investiguer, assurer une cohérence dans les informations communiquées et éviter que l'incident ne se reproduise.

En résumé, il conviendra de :

✓ Déterminer d'où provient la violation de données personnelles (de l'entité cliente ou de l'un des cabinets de commissariat aux comptes ?).

✓ Se concerter avant toute notification à la CNIL ou aux personnes concernées.

Par exemple : perte d'un disque dur externe sur lequel se trouvent des données personnelles non cryptées.

***Attention* : cette concertation ne doit pas avoir pour effet de retarder la notification à la CNIL qui doit se faire dans un délai de 72 heures maximum suivant la découverte de la violation de données.**

✓ Informer sans délai l'entité contrôlée concernée si des données à caractère personnel lui appartenant sont touchées par la violation de données.

✓ Déterminer si une notification aux personnes concernées est nécessaire.

Pour plus d'information sur la notion de violation de données et les cas dans lesquels il est nécessaire de procéder à une notification de ces violations à la CNIL et/ou aux personnes concernées, vous pouvez vous référer aux lignes directrices du CEPD en date du 14 janvier 2021[158].

[158] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

Transferts internationaux

Transferts internationaux

Fiche n° 7

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Transferts internationaux

Synthèse

Cette fiche a pour objectif de vous guider dans l'encadrement des transferts internationaux de données à caractère personnel.

Les pays situés au sein de l'UE, l'EEE[159] ou dans les pays bénéficiant d'une décision d'adéquation de la Commission européenne[160] sont considérés comme offrant un niveau de protection adéquat au sens de la Réglementation applicable. Les transferts vers ces pays ne posent pas de difficulté particulière[161].

En revanche, les transferts vers les autres pays, généralement hors UE ou EEE (ci-après **« Pays Tiers »**) doivent être encadrés, car ils n'assurent pas un niveau de protection adéquat.

Les transferts internationaux de données nécessitent de :

- ✓ Effectuer une cartographie des traitements mis en oeuvre par votre cabinet afin d'identifier les transferts de données personnelles vers des Pays Tiers.
- ✓ Localiser vos sous-traitants (au sens du RGPD) situés dans des Pays Tiers et vérifier que les contrats avec ces derniers comportent des dispositions relatives aux transferts internationaux de données (Cf. Fiche n° 10 du guide *« Gestion des sous-traitants »*).
- ✓ Vérifier le pays de destination et la justification de ce transfert (au besoin en vous faisant assister par votre conseil).
- ✓ Si le pays de destination ne bénéficie pas d'une décision d'adéquation de la Commission européenne, mettre en place l'une des garanties appropriées énumérées à l'article 46 du RGPD à savoir, essentiellement des clauses contractuelles types (CCT) ou des règles d'entreprise contraignantes (aussi appelées *« Binding Corporate Rules »* ou BCR) **(2)**.

[159] Les pays membres de l'EEE sont la Norvège, l'Islande et le Liechtenstein.

[160] En juillet 2021, ces pays sont l'Andorre, l'Argentine, le Canada, les Îles Féroé, Guernesey, Israel, l'Île de Man, le Japon, Jersey, la Nouvelle-Zélande, la Suisse, l'Uruguay et le Royaume-Uni (https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde).

[161] EPour mémoire, l'accès à distance depuis un pays hors UE s'assimile à un transfert hors UE de données personnelles. En effet, la définition de « Traitement » fournie par l'article 4 § 2 du RGPD est suffisamment large pour que la simple consultation de données personnelles, même à distance, soit considérée comme un traitement de données à caractère personnel.

Transferts internationaux

Sommaire

1. La notion de transfert de données à caractère personnel « vers un Pays Tiers »

Qu'est-ce qu'un « transfert international de données » ? Le transfert international de données est défini par la CNIL comme *« toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'union européenne »*[162].

Le commissaire aux comptes peut être amené à réaliser des transferts internationaux de données personnelles :

Par exemple : s'il a recours à un fournisseur de services cloud situé en dehors de l'UE ou encore si son cabinet fait partie d'un réseau international de cabinets de commissaires aux comptes qui partagent entre eux des données personnelles ou des documents contenant des données personnelles, de même s'il a recours à une *hotline* informatique externalisée dans des Pays Tiers tels que l'Inde ou le Maroc.

Dans ce cadre, les règles relatives aux transferts internationaux s'appliquent.

La Règlementation applicable distingue **deux types de transferts internationaux** de données à caractère personnel :

- Les transferts en UE, EEE ou vers des pays bénéficiant d'une décision d'adéquation de la Commission européenne[163] : Ces transferts ne nécessitent pas d'autorisation spécifique puisque le Pays Tiers est reconnu par la Commission européenne comme offrant un niveau de protection adéquat.

> *À noter :* Il convient de consulter régulièrement cette liste car la Commission peut ajouter de nouveaux pays ou au contraire, modifier ou abroger sa décision à l'égard d'un pays lorsqu'elle considère que celui-ci n'assure plus un niveau de protection adéquat.

- Les transferts vers des Pays Tiers : ces transferts doivent être assortis de *« garanties appropriées »,* telles qu'énumérées à l'article 46 du RGPD **(2).**

En tant que responsable de traitement, le commissaire aux comptes doit savoir où se situent les données personnelles qu'il traite ou que traitent ses sous-traitants. Il est donc essentiel d'identifier les transferts de données personnelles vers des Pays Tiers et de veiller à ce que ces transferts présentent les garanties suffisantes pour que le niveau de sécurité ne soit pas compromis ; à savoir la mise en place de clauses contractuelles types, de BCR ou l'adhésion à un Code de conduite.

[162] CNIL « Transfert de données ».

[163] En juillet 2021, ces pays sont l'Andorre, l'Argentine, le Canada, les Îles Féroé, Guernesey, Israel, l'Île de Man, le Japon, Jersey, la Nouvelle-Zélande, la Suisse, l'Uruguay et le Royaume-Uni (https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde).

Comment qualifier le Royaume-Uni après le BREXIT ?

La Commission européenne a adopté le 28 juin 2021 deux décisions d'adéquation vis-à-vis du Royaume-Uni : l'une au titre du règlement général sur la protection des données (RGPD)[164] et l'autre au titre de la directive en matière de protection des données dans le domaine répressif[165].

Les transferts de données personnelles depuis l'Union européenne vers le Royaume-Uni peuvent donc s'effectuer sans encadrement spécifique.

Le site internet de la CNIL est régulièrement mis à jour sur ces questions d'actualité et l'impact en terme d'encadrement des transferts concernés.

Quid des transferts de données personnelles vers les États-Unis ?

Les États-Unis sont considérés comme un pays n'offrant pas un niveau de protection adéquat.

Dans un arrêt en date du 16 juillet 2020[166] (dit « Schrems II »), la Cour de Justice de l'Union Européenne (CJUE) a invalidé la décision d'adéquation 2016/1250 de la Commission européenne dont bénéficiait jusqu'alors le *« EU-US Privacy Shield »*[167].

Dans cette décision, la CJUE a considéré que la législation américaine rendait possible des ingérences par les autorités américaines dans les droits fondamentaux des personnes concernées dont les données sont transférées aux États-Unis sans encadrement ni garanties équivalents à ceux requis par le droit de l'Union Européenne[168].

Par conséquent, **le *Privacy Shield*[169] n'est plus considéré comme garantissant un niveau de protection adéquat.**

Avant même cet arrêt de la CJUE, la CNIL considérait les États-Unis comme n'assurant qu'un niveau de protection partiellement adéquat (Cf. Fiche CNIL *« Carte de la protection des données dans le monde »*).

Dans l'attente des négociations entre les États-Unis et l'Union Européenne (et d'une éventuelle prochaine décision d'adéquation), il convient, **avant** de procéder au transfert, d'effectuer une **analyse des risques** (aussi appelée *« transfer impact assessment »* ou *« TIA »*).

[164] Conformément au règlement (UE) 2016/679.
[165] Conformément à la directive (UE) 2016/68.
[166] CJUE, 16 juillet 2020, C-311/18, Data Protection Commissionner/Maximillian Schrems et Facebook Ireland.
[167] Décision d'adéquation 2016/1250 de la Commission européenne du 12 juillet 2016
[168] Cf. point 184 et 185 de l'arrêt : *« Il apparaît dés lors que ni l'article 702 du FISA ni l'E.O. 12333, lus en combinaison avec la PPD-28 [législation américaine],* ***ne correspondent aux exigences minimales attachées, en droit de l'Union, au principe de proportionnalité,*** *si bien qu'il n'est pas permis de considérer que les programmes de surveillance fondés sur ces dispositions sont limités au strict nécessaire. Dans ces conditions, les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers les États-Unis, et que la Commission a évaluées dans la décision BPD,* ***ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union*** *».*
[169] Le *Privacy Shield* est un mécanisme d'auto-certification entré en vigueur en août 2016 permettant à certaines entreprises américaines d'y adhérer sur la base du volontariat et de s'engager ainsi à assurer un niveau de protection des données européennes qu'elles traitent.

Cette analyse préalable est destinée à évaluer les circonstances du transfert et identifier les mesures complémentaires qui pourraient être mises en place (Cf. Questions-Réponses du CEPD sur le *Privacy Shield*[170]). Selon le résultat de cette évaluation, le transfert devra être encadré par :

- **Une des garanties appropriées énumérées à l'article 46 du RGPD** (clauses contractuelles types, BCR…).
- **Des mesures complémentaires** destinées à garantir que la législation américaine n'empiète pas sur le niveau de protection adéquat des données.

Le CEPD a publié ses recommandations en la matière[171], et préconise notamment de suivre les étapes suivantes :

1. Cartographier les transferts de données personnelles vers des pays tiers et vérifier que seules les données nécessaires au regard de la finalité du traitement sont transférées.
2. Vérifier la garantie appropriée qui encadre le transfert.
3. Évaluer si la législation du pays importateur est susceptible de remettre en cause l'efficacité du mécanisme encadrant le transfert.
4. Identifier et adopter des mesures complémentaires, si l'évaluation menée précédemment révèle que la législation du pays tiers peut remettre en cause l'efficacité du mécanisme encadrant le transfert (les recommandations du CEPD donnent des exemples de mesures complémentaires de type contractuelles, organisationnelles ou techniques par exemple : obligation de transparence et de reporting, chiffrement, localisation des clés de chiffrement en UE, désignation d'un DPO).
5. Effectuer les formalités que peuvent nécessiter la mise en place de ces mesures complémentaires.
6. Procéder à une réévaluation régulière du niveau de protection des données faisant l'objet du transfert.

À noter : L'encadrement des transferts de données personnelles vers les pays non-adéquats (notamment les États-Unis) est un sujet d'actualité à suivre de près. Il est recommandé aux cabinets de commissariat aux comptes de se tenir informés des dernières évolutions sur ce point en se rendant sur le site internet de la CNIL et du CEPD.

La vigilance s'impose également au regard des entreprises américaines soumises au *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* qui permet à la justice américaine, sous certaines conditions, d'obtenir la communication de données personnelles hébergées

[170] Questions-Réponses du CEPD, réponse à la question : *« Que vous puissiez ou non transférer des données personnelles sur la base des CCT dépendra du résultat de votre évaluation, qui tiendra compte des circonstances des transferts, et des mesures supplémentaires que vous pourriez mettre en place. L'ensemble formé par les mesures supplémentaires et les CCT,* ***après une analyse au cas par cas des circonstances entourant le transfert,*** *devra garantir que la législation américaine ne compromet pas sur le niveau de protection adéquat que les clauses et ces mesures garantissent ».*

[171] EDPB – final version of the Recommendations on supplementary measures to ensure compliance with the EU level of protection of personal data – Adopted on 21 June 2021 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

par ces entreprises, y compris lorsque cet hébergement est effectué en dehors des États-Unis et notamment en Europe.

- **Avant d'effectuer un transfert de données personnelles vers les États-Unis, il convient donc de :**

✓ Effectuer **en amont** du transfert une analyse des risques au cas par cas, afin d'évaluer les circonstances du transfert.

✓ S'assurer que le transfert est conforme aux grands principes de la Règlementation applicable (information des personnes concernées, respect du principe de minimisation, sécurité des données, conservation limitée, etc.).

✓ Déterminer si l'entreprise réceptrice agit en tant que sous-traitant ou en tant que responsable du traitement.

✓ Encadrer le transfert par l'une des garanties appropriées de l'article 46 (telles que des Clauses contractuelles types par exemple) et des mesures complémentaires préconisées par le CEPD.

- **Les bonnes pratiques en matière de transferts hors UE/EEE/vers des Pays Tiers :**

✓ Effectuer une cartographie des traitements mis en œuvre par votre cabinet afin d'identifier les transferts de données personnelles vers des Pays Tiers (Cf. Fiche CNCC sur le RGPD n° 4 *« RGPD : Réalisez une cartographie des données collectées et de leurs traitements »*[172] et Fiche 1 du guide *« Gouvernance et accountability »*).

✓ Localiser vos sous-traitants situés dans un Pays Tiers, notamment les hébergeurs (Cf. Fiche de la CNCC sur le RGPD n° 5 *« Sécurisez vos relations avec vos prestataires »*) et vérifier que les contrats avec ces derniers comportent des dispositions relatives aux transferts internationaux de données (Cf. Fiche n° 10 du guide *« Gestion des sous-traitants »*).

✓ Vérifier le pays de destination des données personnelles et la base légale ou contractuelle de ce transfert.

✓ Si le pays de destination ne bénéficie pas d'une décision d'adéquation de la Commission européenne, mettre en place les garanties appropriées énumérées à l'article 46 du RGPD **(2)**.

À noter : Vous devez vous assurer que les personnes concernées ont été informées du transfert de leurs données personnelles vers des Pays Tiers. Cela doit être indiqué dans votre politique de confidentialité, vos conditions générales d'intervention et/ou votre lettre de mission.

[172] *« Action #1 Formalisez une cartographie précise des données collectées et de leurs traitements (…) Cet état permet d'établir un premier aperçu* ***reprenant*** *par exemple (…) l'emplacement de stockage, l'emplacement de sauvegarde, les transferts hors UE (…) ».*

2. Les garanties à mettre en place en cas de transfert vers un Pays Tiers

Transférer des données vers un pays tiers n'est pas en soi interdit. Le recours à un sous-traitant ou un autre responsable du traitement situé dans un pays tiers n'est pas problématique dès lors que ce transfert est encadré par l'une des garanties appropriées énumérées à l'article 46 du RGPD, à savoir les règles d'entreprise contraignantes **(2.1),** les clauses contractuelles types **(2.2)** ou un Code de conduite approuvé **(2.3).**

2.1 Les règles d'entreprise contraignantes (BCR)

Les règles d'entreprise contraignantes, aussi appelée « BCR » *(Binding Corporate Rules)* sont définies par la Commission européenne comme *« un mécanisme de transfert développé par les autorités nationales chargées de la protection des données auquel les organisations privées peuvent recourir dans le cadre de leurs échanges de données à caractère personnel* ***entre entités faisant partie de la même organisation*** *»*[173].

Selon la CNIL *« Les règles d'entreprise contraignantes (BCR) ne sont pas uniquement un outil d'encadrement des transferts de données personnelles hors de l'Union européenne,* ***elles constituent une véritable politique de conformité et de protection des données intra-groupe,*** *applicables à toutes les entités d'un groupe qui adhèrent à ce dispositif »*[174].

Ainsi, les règles d'entreprise contraignantes constituent à la fois un outil juridique destiné à régir les transferts internationaux de données personnelles effectués au sein d'un groupe ou d'un réseau d'entreprises mais aussi une politique globale de gouvernance des données au sein de ce groupe.

Comme le rappelle la CNIL, cet outil est avant tout utilisé par des grands groupes ou des multinationales effectuant de nombreux transferts de données entre leurs entités situées partout dans le monde (Cf. Fiche de la CNIL *« Ce qu'il faut savoir sur les BCR »*, rubrique *« Quelles entreprises sont concernées par les BCR ? »*).

Par exemple : Au sein d'un cabinet d'audit international disposant de bureaux en France et à l'étranger, les BCR peuvent être utilisées pour encadrer les transferts de données à caractère personnel entre les différentes entités ou membres du réseau.

> *À noter :* Les règles d'entreprise contraignantes font partie de la documentation « data privacy » à conserver et tenir à jour dans le cadre du respect du principe d'*accountability* (Cf. Fiche n° 1 du guide *« Gouvernance et accountability »*). Elles doivent être approuvées par la CNIL et le CEPD à l'issue de la procédure d'approbation.

[173] https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_fr.
[174] Fiche CNIL « Comment préparer un dossier de BCR ? ».

Il existe deux types de BCR :

- **Les BCR « responsable du traitement »** s'appliquent aux transferts de données entre un responsable du traitement établi dans l'UE et d'autres entités de son groupe établies hors de l'UE, agissant en tant que responsable du traitement ou sous-traitant.
- **Les BCR « sous-traitant »** encadrent les transferts de données entre les différentes entités du groupe agissant en qualité de sous-traitant.

Pour plus d'information, consultez la fiche de la CNIL *« Pourquoi mettre en place des BCR ? »*, rubrique *« Des BCR responsable de traitement et sous-traitant »* ainsi que les Lignes directrices du CEPD relatives aux BCR sous-traitants.

Que contiennent ces BCR et comment les rédiger ?

Les BCR doivent contenir les 14 éléments listés à l'article 47 du RGPD, à savoir notamment :

- Les droits des personnes concernées et les moyens d'exercer ces droits.
- Les catégories de données personnelles.
- Le type de traitement.
- Les finalités du traitement.
- Le type de personnes concernées.
- Le nom du ou des Pays Tiers en question.

Dans sa fiche « Comment préparer un dossier de BCR », la CNIL indique les différentes étapes et actions à mener dans le cadre de la rédaction de BCR et la préparation du dossier d'instruction, jusqu'à la soumission du projet à la CNIL (Pour plus d'informations, vous pouvez consulter la fiche de la CNIL *« Soumettre un dossier d'approbation BCR à la CNIL »*).

Quels sont les avantages des BCR ?

Les BCR permettent de ne pas conclure de contrat pour chaque transfert de données à caractère personnel effectué au sein d'un groupe. Les BCR représentent également un gage de confiance pour les clients et un outil d'harmonisation de la protection des données personnelles au sein d'un groupe. La procédure de mise en place demeure cependant assez longue (Cf. Fiche de la CNIL *« Approbation des BCR : les différentes étapes »*).

2.2 Les Clauses Contractuelles Types (CCT)

Les clauses contractuelles types sont des modèles de contrats adoptés par la Commission européenne relatifs aux transferts de données vers des Pays Tiers. Elles intègrent des stipulations générales et des stipulations particulières divisées en quatres modules applicables selon que les données sont transférées entre responsables du traitement (module 1), de responsable du traitement à sous-traitant (module 2), entre sous-traitants (module 3) ou encore de sous-traitant à responsable de traitement (module 4). Ces CCT sont évolutives.

Cas pratique :

Dans le cadre d'appels d'offres de grands groupes internationaux, il arrive que l'entité contrôlée demande à ses commissaires aux comptes de signer des clauses contractuelles types (de responsable du traitement à responsable du traitement) en considérant que le transfert des données vers le commissaire aux comptes constitue un « traitement » à part entière (ce qui est contestable). Il convient de préciser que la signature de ces clauses n'est pas nécessaire si votre cabinet dispose de règles d'entreprise contraignantes (cf. point 2.1). En outre, en toute hypothèse, il faut veiller à ce que la signature des clauses contractuelles types ne remette pas en question le statut de responsable du traitement du commissaire aux comptes.

2.3 Le Code de conduite

Le Code de conduite est un outil d'*accountability* juridiquement contraignant prévu à l'article 40 du RGPD[175]. A la différence des BCR qui s'appliquent au sein d'un groupe d'entreprises, le Code de conduite est élaboré par les représentants (responsables du traitement ou sous-traitants) d'un secteur d'activité et s'applique à l'ensemble des adhérents. Il a vocation à constituer un socle commun des bonnes pratiques mises en place au sein d'un secteur donné en matière de données personnelles et à faciliter l'application de la Règlementation applicable au sein de celui-ci.

Pour en savoir plus, vous pouvez consulter la fiche de la CNIL « Ce qu'il faut savoir sur le Code de conduite » et aux lignes directrices du CEPD relatives aux Codes de conduite.

Le Code de conduite doit être approuvé à l'issue d'une procédure d'approbation au niveau national par la CNIL ou au niveau européen par la Commission européenne (lorsque le projet concerne des activités de traitement menées dans plusieurs États membres). Le Code n'est approuvé que si l'autorité compétente estime qu'il offre des garanties appropriées suffisantes. Là encore la procédure d'approbation est longue.

À noter : Procéder à un transfert de données personnelles en dehors de l'UE sans mettre en place les garanties précitées constitue **un délit pénal puni de 5 ans** d'emprisonnement et de **300 000 euros d'amende[176],** en sus des sanctions administratives pouvant être prises par la CNIL[177].

[175] Article 40 du RGPD : *« Les États-membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de Codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises ».*

[176] En application de l'article 131-38 du Code pénal, le montant de l'amende peut être porté au quintuple pour une personne morale.

[177] Article 226-22-1 du Code pénal : *« Le fait de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à l'Union européenne ou à une organisation internationale en violation du chapitre V du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril (…) ou des articles 112 à 114 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».*

2.4 Les mécanismes de certification

Les mécanismes de certification approuvés font partie des garanties appropriées énumérées à l'article 46 § 2 f) du RGPD en matière de transferts de données vers des Pays tiers.

L'article 42 du RGPD dispose que « Les États-membres, les autorités de contrôle, le comité et la Commission **encouragent,** en particulier au niveau de l'Union, la mise en place de **mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière,** aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement ».

Le mécanisme de certification constitue **un engagement contraignant et exécutoire** pris par les destinataires hors UE d'appliquer les garanties appropriées prévues à l'article 46 du RGPD dans le cadre de transferts internationaux de données.

Ces mécanismes de certification doivent être approuvés par l'autorité de contrôle compétente (en France, la CNIL) et les organismes de certifications agréés[178]. La certification délivrée à un responsable du traitement ou à un sous-traitant est valable pour une durée de trois ans renouvelables[179].

Pour l'heure, cette garantie appropriée n'est pas encore opérationnelle. À notre connaissance il n'existe pas encore de mécanisme de certification mis en place en matière de transferts internationaux de données personnelles au niveau national ou européen.

3. Les cas dérogatoires permettant des transferts sans mise en œuvre de ces garanties

L'article 49 du RGPD prévoit des cas dérogatoires dans lesquels le transfert vers un Pays Tiers peut avoir lieu sans la mise en œuvre de garanties appropriées.

Cependant, ces situations n'ont pas vocation à s'appliquer au commissaire aux comptes s'agissant de données traitées dans le cadre de sa mission (le commissaire aux comptes n'ayant pas contracté directement avec les personnes concernées mais avec l'entité contrôlée).

Pour plus d'informations, vous pouvez consulter la fiche de la CNIL *« Transfert de données hors UE – Dérogations pour des situations particulières »*

*****

Annexe – Clauses contractuelles types

Les Clauses contractuelles types suivantes s'appliquent depuis le 4 juin 2021 :

- Version FR
- Version ENG

[178] Article 42.5 et 43 du RGPD.
[179] Article 42.7 du RGPD.

Sécurité des données

Sécurité des données

Fiche n° 8

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

En tant que responsable du traitement, le commissaire aux comptes est tenu à une obligation de sécurité et protection des données personnelles qu'il traite (**1**).

Le commissaire aux comptes doit être en mesure de démontrer que les données personnelles qu'il traite le sont de manière sécurisée[180] (**2**). Cela implique de sa part de :

- ✓ Informer et se former régulièrement aux sujets de sécurité.
- ✓ Mettre en place des mesures de sécurité techniques et organisationnelles, les documenter et veiller à leur mise à jour régulière.
- ✓ Effectuer une revue régulière des mesures de sécurité (telles que la réalisation d'audits sécurité, les tests d'intrusion, la mise à jour de la documentation, etc.) et d'en conserver la trace, de même que des actions correctrices menées (le cas échéant).
- ✓ Faire preuve de vigilance dans le recrutement et la gestion de ses sous-traitants en s'assurant que le contrat de sous-traitance prévoit bien des obligations de sécurité à leur charge (Cf. Fiche n° 10 du guide *« Gestion de la sous-traitance »*), en particulier lorsque ceux-ci sont établis à l'étranger.

La sécurité étant également un sujet important pour les entités contrôlées, le commissaire aux comptes peut être amené à être interrogé sur ces questions. Sur le plan contractuel, il devra être prudent dans les réponses apportées aux questionnaires de sécurité adressés par ces entités ou aux demandes d'audit (3).

L'obligation de sécurité des données personnelles revêt une importance croissante, comme l'illustrent les sanctions prononcées par la CNIL ces dernières années : les manquements à l'obligation de sécurité sont systématiquement sanctionnés (**1.2**). Il est donc essentiel d'observer les règles à suivre pour éviter les cas de violations de données (**0**).

Une synthèse des principales mesures de sécurité recommandées par la CNIL dans son guide de sécurité de la CNIL (édition 2018) figure à la fin de la présente fiche 8.

[180] Article 5.2 du RGPD : *« Le responsable du traitement est responsable du respect du paragraphe 1 et est **en mesure de démontrer** que celui-ci est respecté (responsabilité) ».*

Sécurité des données

Sommaire

1. L'obligation de sécurité : nature et sanctions

1.1 Principes

La Loi informatique et libertés[181] et le RGPD[182] imposent aux responsables du traitement et aux sous-traitants une obligation de sécurité des données à caractère personnel.

Au regard des délibérations de la CNIL, l'obligation de sécurité des données constitue plutôt une obligation de moyens[183]. En effet, les termes de l'article 32 du RGPD rappellent ceux d'une obligation de moyens. En revanche, certains engagements de sécurité, s'ils sont précis et mesurables, peuvent constituer un engagement de résultat (exemple : mettre en œuvre des mots de passe robustes et conformes aux préconisations de la CNIL, maintenir une certification de sécurité…).

En tant que responsable du traitement, le commissaire aux comptes doit mettre en place au sein de sa structure les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données personnelles qu'il traite.

Ces mesures doivent permettre de garantir la confidentialité des données en les protégeant contre la perte, la destruction, l'accès non-autorisé par des tiers et plus généralement contre les violations de données à caractère personnel.

Les mesures de sécurité doivent être déterminées en considération *« de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques dont le degré de probabilité et de gravité varie »*. Cela signifie notamment que les mesures de sécurité doivent être renforcées en ce qui concerne les catégories particulières de données.

Par exemple : Si dans le cadre de ses missions, le commissaire aux comptes se voit confier un fichier comportant les NIR[184] de plusieurs salariés de l'entité contrôlée, il doit veiller à ce que ce fichier fasse l'objet d'un niveau de sécurité approprié au sein de son système d'information.

L'article 32 § 2 du RGPD invite le responsable du traitement à faire une *« évaluation du niveau de sécurité approprié »* en tenant compte en particulier des risques que présente le traitement[185].

---

[181] Article 4 § 6 de la Loi informatique et liberté : *« Les données à caractère personnel doivent être traitées de façon à **garantir une sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de **mesures techniques ou organisationnelles appropriées** ».*

[182] Article 32 du RGPD : *« (…) le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…) ».*

[183] CNIL Délibération n° 2014-298 du 7 août 2014 : *« l'obligation de notifier une violation de données, obligation de résultat à laquelle la société a satisfait, est distincte de celle relative à la sécurité et la confidentialité des données, obligation de moyens ».*

[184] Pour rappel, le NIR ou « numéro de sécurité sociale » fait partie selon la CNIL des données qui doivent bénéficier d'une « protection particulière » (Cf. Fiche CNIL *« Vérifier la pertinence des données »*).

[185] Article 32 § 2 du RGPD « *Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou de l'accès non-autorisé à de telles données, de manière accidentelle ou illicite ».*

À noter : une bonne protection des données consiste également à ne collecter que celles dont vous avez strictement besoin pour vos missions (principe de minimisation) et à les supprimer à l'expiration des durées de conservation (principe de conservation limitée).

1.2 Sanctions

Les manquements à l'obligation de sécurité peuvent faire l'objet :

- d'une amende administrative pouvant s'élever au montant le plus élevé entre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial[186] ;
- de sanctions pénales (300 000 euros d'amende et 5 ans d'emprisonnement)[187], étant précisé que ce montant peut être porté au quintuple pour les personnes morales[188] ;
- de sanctions civiles telles que des dommages-intérêts en cas de préjudice causé à une personne.

Les dernières délibérations de la CNIL montrent que les manquements à l'obligation de sécurité sont systématiquement sanctionnés.

Exemples de manquements sanctionnés :

- L'absence de procédure d'authentification des utilisateurs. En l'espèce, la société, qui avait connaissance de cette faille, a mis 6 mois à mettre en place les correctifs nécessaires. La CNIL a considéré qu'il s'agissait d'un manquement aggravé et l'a condamnée au paiement d'une amende de 400 000 euros[189].
- L'absence de mise en place de dispositif permettant d'éviter la prévisibilité des URL. En l'espèce, une simple modification de l'URL du formulaire de collecte permettait à des tiers d'accéder aux documents des utilisateurs du site web tels que des avis d'imposition, des pièces d'identité, bulletins de salaires, etc. L'association a été condamnée au paiement d'une amende d'un montant de 75 000 euros[190].
- Le manque de robustesse des mots de passe d'accès, combiné à l'absence de verrouillage automatique de la session au-delà d'une période d'inactivité[191]. En l'espèce, la société a été condamnée au paiement d'une amende de 10 000 euros.
- Le stockage en clair des identifiants d'accès aux serveurs dans un fichier non-protégé et l'absence de processus relatif au retrait des habilitations des anciens salariés ayant quitté la société[192]. En l'espèce, la société a été condamnée au paiement d'une amende de 400 000 euros.

[186] Article 20 de la loi informatique et libertés, article 83 du RGPD.
[187] Article 226-17 du Code pénal *« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites aux articles (…) 32 du règlement UE 2016/679 du 27 avril 2016 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende »*.
[188] Article 131-38 du Code pénal *« Le taux maximum de l'amende applicable aux personnes morales est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction »*.
[189] CNIL Délibération du 28 mai 2019 n° SAN 2019-005.
[190] CNIL Délibération du 21 juin 2018 n° SAN 2018-003.
[191] CNIL Délibération du 6 septembre 2018 n° SAN 2018-009.
[192] CNIL Délibération du 19 décembre 2018 n° SAN 2018-011.

2. Encadrer et documenter les processus de sécurité en place

Le principe d'*accountability* impose au responsable du traitement d'**être en mesure de démontrer** qu'il a mis en œuvre les mesures appropriées pour assurer la sécurité des données. Autrement dit, la mise en place des mesures techniques et organisationnelles de sécurité doit être **documentée** (Cf. Fiche n° 1 du guide *« Gouvernance et accountability »*).

Cette documentation est susceptible de vous être demandée en cas de contrôle CNIL (Cf. Fiche n° 9 du guide *« Contrôles et sanctions de la CNIL »*).

Par exemple : les agents de la CNIL peuvent vous demander de fournir une copie des contrats de sous-traitance, de votre charte informatique, vérifier la procédure d'authentification pour l'accès à vos outils…

• Les bonnes pratiques à mettre en œuvre :

✓ Sensibiliser et former vos collaborateurs et salariés à la sécurité des données personnelles (Charte informatique, clause de confidentialité, formations, etc. Cf. Fiche CNIL *« Sécurité : sensibiliser les utilisateurs »*).

✓ Effectuer une revue régulière des mesures de sécurité (audits de sécurité, tests d'intrusion, mise à jour des processus en place au vu des évolutions de l'état de l'art en matière de sécurité, etc.) et en conserver la trace et évaluer son niveau de sécurité[193].

✓ Documenter la mise en place des mesures de sécurité techniques et organisationnelles et les mettre à jour régulièrement (Cf. tableau de synthèse). Pour les cabinets d'une certaine taille, l'obtention de certifications de type ISO/IEC 27000-27799, en particulier les normes 27001 et 27017 peut présenter un gage de fiabilité supplémentaire.

✓ Se doter d'une procédure sur la marche à suivre en cas de violation de données personnelles (Cf. Fiche n° 6 du guide *« Le RGPD dans un contexte co-CAC »*).

✓ Identifier les données et traitements nécessitant une attention particulière en termes de sécurité (Cf. Fiche n° 1 du guide *« Gouvernance et accountability »* voir paragraphes 2.2 et 3.2 sur l'importance de cartographier ses traitements).

À noter : La CNIL préconise une approche par les risques en recommandant aux responsables du traitement de s'interroger en amont sur les risques pour la vie privée des personnes concernées engendrés par le traitement afin de déterminer les moyens à mettre en œuvre pour réduire ces risques (Cf. Fiche de la CNIL *« Garantir la sécurité des données »*).

✓ Pour les traitements qui le nécessitent, effectuer une analyse d'impact préalable à la mise en œuvre du traitement[194].

✓ Identifier et encadrer les transferts de données vers des pays ne bénéficiant pas de décision d'adéquation (Cf. Fiche n° 7 du guide *« Transferts internationaux »*).

[193] https://www.cnil.fr/sites/default/files/atoms/files/check_list_0.pdf

[194] Article 62 de la loi informatique et libertés, article 35 du RGPD. La CNIL met à disposition un logiciel *open source* pour vous accompagner dans la réalisation d'analyses d'impact
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

✓ Faire preuve de vigilance dans le recrutement et la gestion des sous-traitants notamment en vous assurant que le contrat de sous-traitance prévoit bien des obligations de sécurité adaptées (Cf. Fiche n° 10 du guide *« Gestion de la sous-traitance »*).

Rappel : En tant que responsable du traitement, vous pouvez être tenu responsable à l'égard des personnes concernées ou de tiers des manquements de vos sous-traitants.

Le tableau de synthèse évoqué dresse une liste des mesures de sécurité techniques et organisationnelles à mettre en place *a minima*, telles que figurant dans la dernière version du guide de sécurité publié par la CNIL (version 2018).

3. La sécurité dans les rapports contractuels du commissaire aux comptes avec les entités contrôlées (questionnaires de sécurité & audits)

Certaines entités contrôlées souhaitent être rassurées sur les mesures de sécurité mises en place par les entreprises auxquelles elles confient leurs données, et ce, indépendamment de tout débat sur la qualification de « responsable du traitement » ou de « sous-traitant » au sens de la Réglementation applicable.

Il arrive ainsi que des entités contrôlées demandent au commissaire aux comptes de les informer sur les mesures de sécurité mises en place au sein de son cabinet, en amont de ou pendant toute la durée de la mission qui lui est confiée, y compris s'agissant de l'archivage des dossiers traités.

Ces vérifications se traduisent le plus souvent par des demandes de réponses à des questionnaires de sécurité (par exemple dans le cadre d'une réponse à un appel d'offres) ou des demandes d'audit des mesures de sécurité mises en œuvre par le commissaire aux comptes.

Le commissaire aux comptes étant responsable des traitements de données personnelles et non « sous-traitant », il convient de rappeler qu'il n'existe aucune obligation légale de répondre à des questionnaires détaillés ou faire droit à une demande d'audit de la part d'une entité contrôlée. En revanche, le commissaire aux comptes peut accepter d'y répondre sous certaines conditions (voir ci-après concernant les demandes d'audit).

S'agissant des questionnaires de sécurité, il faut faire preuve de vigilance quant aux réponses apportées. **Des réponses trop détaillées peuvent compromettre la sécurité si elles révèlent des informations confidentielles sur des éléments d'architecture technique ou mécanismes de protection en place.**

De même, il est nécessaire d'être vigilant à l'égard de certains clients qui peuvent exiger un renforcement des engagements contractuels lorsque le commissaire aux comptes n'est pas en mesure de répondre à des exigences de sécurité spécifiques, telle que le cryptage des données par exemple.

Exemple de mention d'accompagnement en réponse à un questionnaire de sécurité :

Les réponses apportées par notre cabinet à ce questionnaire sont fournies à titre strictement confidentiel et informatif, compte tenu des mesures en vigueur. Il est possible que certaines rubriques ne soient pas renseignées si nous estimons que la fourniture des informations demandées est de nature à compromettre les mesures de sécurité mises en place au sein de notre cabinet. Nous définissons seuls les mesures de sécurité techniques et organisationnelles appropriées au regard des traitements de données à caractère personnel opérés et plus généralement des documents confidentiels traités dans le cadre de notre mission. Ce questionnaire ne constitue donc en aucun cas des instructions de la part de l'entité contrôlée à notre égard. Notre cabinet est et demeure seul responsable des traitements de données à caractère personnel réalisés dans le cadre de la mission confiée.

Concernant les demandes d'audit, comme énoncé ci-avant le commissaire aux comptes, en tant que responsable du traitement, n'est pas tenu par une obligation légale de faire droit à une telle demande de la part d'une entité contrôlée.

En revanche, le commissaire aux comptes peut accepter de se livrer à cet exercice sous certaines conditions :

- ✓ **L'audit ne doit jamais contrevenir aux obligations déontologiques et professionnelles propres au commissaire aux comptes**, ni contrevenir par exemple à la préservation du secret professionnel. Il est rappelé que l'entité contrôlée (et *a fortiori* son auditeur) ne peut délier le commissaire aux comptes de son secret professionnel, lequel a un caractère absolu.
- ✓ **L'audit doit être limité dans son périmètre** (uniquement la sécurité des données propres à l'entité contrôlée) et sa fréquence. L'audit ne peut en aucun cas porter sur le contenu du dossier de travail du commissaire aux comptes (que ce soit celui de l'entité contrôlée ou de toute autre entité).
- ✓ Par ailleurs, comme pour tout audit, il est recommandé que celui-ci soit réalisé **aux frais du client**, en respectant un préavis raisonnable, que l'auditeur désigné soit indépendant (non concurrent du commissaire aux comptes) et tenu par un engagement de confidentialité renforcé.

Il est préférable et recommandé de privilégier un audit documentaire par rapport à un audit sur place, qui s'appuiera sur la production d'attestations et/ou rapports de synthèse des mesures de sécurité en place au sein du cabinet. Il est donc essentiel de documenter les mesures de sécurité en place en anticipation d'un audit réalisé par une entité contrôlée.

Le fait de pouvoir disposer de ces éléments à jour et de manière permanente est un gage de confiance qui permet de limiter le temps consacré aux réponses à ces demandes d'audit. Ces demandes d'audit représentent en effet un coût interne à prendre en compte par le cabinet.

Si vous avez obtenu des certifications de sécurité, vous pouvez proposer alternativement de fournir régulièrement une attestation de votre conformité aux normes de sécurité qui vous sont applicables (par exemple : fourniture du certificat de la norme ISO 27000 en cours de validité). Ce mécanisme est moins intrusif que l'audit.

De manière générale, il ne faut pas perdre de vue que **le commissaire aux comptes est et demeure responsable des traitements de données personnelles opérés dans le cadre de sa mission et n'a pas d'instruction à recevoir** de l'entité contrôlée en matière de sécurité des données.

Quid en cas de mise à disposition d'un outil par l'entité contrôlée ?

Lorsqu'un outil de partage de fichiers est mis à disposition du commissaire aux comptes par l'entité contrôlée, celle-ci demeure responsable de la sécurité de cette solution sous réserve du respect par le commissaire aux comptes des règles d'utilisation de l'outil (par exemple, gestion des droits d'accès des collaborateurs respectifs, respect des règles relatives à la robustesse des mots de passe…).

Pour sa part, le commissaire aux comptes demeure responsable de la sécurité des fichiers qui lui ont été transmis par l'entité contrôlée.

4. La gestion des violations de données à caractère personnel

La violation de données est définie comme *« une violation de sécurité entrainant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données »*[195].

La notion de violation de données recouvre **un large panel de situations**, il peut s'agir notamment de :

- Un acte **malveillant** émanant d'un tiers.

  Par exemple : *Ransomware*[196], intrusion non autorisée dans un système d'information par un tiers en vue de divulguer des données personnelles[197].

- Un acte accidentel.

  Par exemple : envoi par erreur d'un fichier client à des destinataires qui n'auraient pas dû recevoir ce fichier (divulgation de données à des tiers non-autorisés).

- Une situation affectant un **sous-traitant** du responsable du traitement.

  Par exemple : votre fournisseur de cloud vous informe qu'il a subi une cyberattaque de ses serveurs contenant des données personnelles traitées par votre cabinet.

[195] Article 4 § 12 du RGPD.

[196] Pour plus d'informations sur les *ransonware*, consultez le guide de l'ANSSI *« Attaque par ransonware, tous concernés : Comment les anticiper et réagir en cas d'incident » (août 2020)*.

[197] La CNCC a souscrit un contrat de cyber-assurance qui peut s'appliquer en cas de cyber-attaque. Nous vous invitons à prendre connaissance des termes de ce contrat et à apprécier si votre activité nécessite une couverture complémentaire. Pour plus d'informations, consultez la fiche CNCC *« Cyber-attaque se protéger et que faire en cas d'attaque »* (avril 2020).

Dans ses lignes direcrices 01/2021 du 14 janvier 2021, le CEPD fournit des exemples pratiques permettant d'illustrer des cas de violations de données au sens du RGPD (*ransomware*, vol de matériel, envoi par erreur de données sensibles par email…), les actions à mettre en œuvre à titre préventif, curatif et les notifications à opérer auprès de la CNIL et, le cas échéant, des personnes concernées[198].

• **Rappel des règles en matière de violations de données à caractère personnel :**

✓ Les données personnelles doivent être traitées de manière à leur garantir **un niveau de sécurité approprié**. Le responsable du traitement est débiteur d'une obligation de sécurité. Il doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir aux données un niveau de sécurité adapté au risque[199] : ainsi il appartient à chaque commissaire aux comptes de mettre en place les mesures adaptées.

✓ La Règlementation applicable impose au responsable du traitement de **notifier toute violation de données à caractère personnel à la CNIL**, à moins que celle-ci ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées[200].

Par exemple : l'envoi par erreur d'un email à un destinataire interne au sein du cabinet contenant un nombre limité de données personnelles de tiers représenterait un risque très limité pour la personne concernée (pas de données sensibles, destinataire interne).

✓ Cette notification doit contenir **les informations énumérées à l'article 33 § 3 du RGPD** (la nature de la violation, les catégories et le nombre approximatif de personnes concernées, etc.). Cela requiert de documenter en interne la violation de données[201] (Cf. Fiche de la CNIL *« Notifier une violation de données personnelles »*).

✓ La notification à la CNIL doit être effectuée *via* le télé service de notification des violations accessible sur le site de la CNIL[202] **dans les meilleurs délais et en tout état de cause dans les 72 heures** suivant la constatation de la violation.

À noter : cette déclaration peut être complétée dans un second temps si vous ne disposez pas de toutes les informations nécessaires ou si des investigations sont en cours.

[198] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

[199] **Article 32 § 1 du RGPD :** *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…) ».*

[200] **Article 33 du RGPD :** *« En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55 dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques ».*

[201] **Article 33 § 5 du RGPD :** *« Le responsable du traitement documente toute violation de données à caractère personnel en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier ».*

[202] https://notifications.cnil.fr/notifications/index

- ✓ Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit en informer les personnes concernées dans les meilleurs délais en des termes clairs et simples[203]. Cette communication doit contenir *a minima* les informations énumérées à l'article 33 § 3 du RGPD.

  Par exemple : L'envoi par erreur d'un fichier comportant les noms, prénoms et rémunérations de l'ensemble des salariés.

- ✓ Il est recommandé de tenir un **registre des violations de données personnelles**[204] indiquant la nature de la violation, les catégories et le nombre approximatif de personnes concernées et de fichiers concernés, les conséquences probables de la violation, les mesures prises pour remédier à la violation ou limiter ses conséquences négatives, le cas échéant la justification de l'absence de notification auprès de la CNIL ou d'information des personnes concernées[205].

- ✓ Comme l'indiquent les Lignes directrices du CEPD en la matière, il recommandé de se doter **d'une procédure/politique interne de gestion des violations** de données afin de savoir à l'avance comment réagir en pareille situation :

« Il est important qu'une fois détectée, une violation soit communiquée au niveau de direction approprié afin qu'il soit possible d'y remédier et, le cas échéant, de la notifier conformément à l'article 33 et, si nécessaire, à l'article 34. De telles mesures et de tels mécanismes de notification devraient être détaillés dans le plan de réaction aux incidents et/ou dans les accords de gouvernance. Ceux-ci aideront le responsable du traitement à planifier et à déterminer efficacement à qui échoit la responsabilité opérationnelle au sein de l'organisation concernant la gestion d'une violation, ainsi que s'il faut, et comment, rapporter une violation de façon appropriée »[206]. Pour plus d'informations, vous pouvez consulter la fiche de la CNIL « Les violations de données personnelles » ou les lignes directrices du CEPD du 14 janvier 2021 qui fournissent des exemples de violations de données sous forme de cas pratiques[207].

À noter : le fait de manquer à son obligation de notifier une violation de données à caractère personnel à la CNIL ou aux personnes concernées constitue un **délit pénal** passible de 5 ans d'emprisonnement et de 300 000 euros d'amende[208] (le montant de cette amende pouvant être porté au quintuple lorsque le prévenu est une personne morale).

[203] **Article 34 du RGPD :** *« Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais ».*

[204] **Lignes directrices du CEPD du 6 février 2018 sur les violations de données à caractère personnel :** *« Les responsables du traitement sont donc encouragés à établir un registre interne des violations, qu'ils soient tenus de les notifier ou non. Le responsable du traitement peut décider de documenter les violations dans le cadre de son registre des activités de traitement tenu conformément à l'article 30. Un registre séparé n'est pas nécessaire, à condition que les informations concernant les violations soient clairement identifiables en tant que telles et puissent être extraites sur demande ».*

[205] Cf. Fiche de la CNIL *« Les violations de données »* rubrique *« Que doit contenir le registre des violations de données ? ».*

[206] **Lignes directrices du CEPD du 6 février 2018 sur les violations de données à caractère personnel, page 13**.

[207] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

[208] Article 226-17-1 du Code pénal *« le fait pour un responsable du traitement de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL ou à l'intéressé en méconnaissance des articles 33 et 34 du règlement UE 2016/679 du 27 avril 2016 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».*

5. Tableau des mesures de sécurité techniques et organisationnelles[209]

Le tableau ci-dessous a pour objet de présenter les principales mesures de sécurité requises a minima par la CNIL. La colonne de droite est à remplir au cas par cas par le cabinet.

	Mesures de sécurités techniques et organisationnelles	**Résumé des mesures** *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	**Documents de référence – Date** [210]
1	Sensibilisation des utilisateurs[211]	• Sensibiliser les utilisateurs (informations effectuées). • Documentation des procédures d'exploitation. • Charte informatique avec valeur contraignante. • Signature d'un engagement de conformité par chaque salarié. • Les nouveaux contrats de travail contiennent une clause de confidentialité spécifique concernant la protection des données personnelles. • Formation CNIL du point de contact données personnelles.	
2	Authentification des utilisateurs (Reconnaître ses utilisateurs pour pouvoir leur donner les accès nécessaires)	• **Définir un identifiant unique par utilisateur et interdire les comptes partagés** entre plusieurs utilisateurs. Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, exiger une validation de la hiérarchie et mettre en œuvre des moyens pour les tracer. • **Respecter la recommandation de la CNIL dans le cas d'une authentification des utilisateurs basée sur des mots de passe**, notamment en stockant les mots de passe de façon sécurisée et en appliquant les règles de complexité suivantes pour le mot de passe : – Au moins **8 caractères comportant 3 des 4 types de caractères** (majuscules, minuscules, chiffres, caractères spéciaux) si l'authentification prévoit une restriction de l'accès au compte (cas le plus courant) comme une temporisation d'accès au compte après plusieurs échecs, un « Captcha » ou un verrouillage du compte après 10 échecs. – **12 caractères minimum et 4 types de caractères** si l'authentification repose uniquement sur un mot de passe.	

[209] Le présent tableau n'est pas exhaustif. Par ailleurs, les mesures de sécurité doivent être adaptées aux risques propres à chaque traitement (nature des données, etc.).
[210] Faire référence à la documentation technique interne du Cabinet (si elle existe) qui permet de justifier que ces mesures sont prises en compte et préciser la dernière date de mise à jour du document référencé.
[211] Cliquer sur le titre pour accéder à la fiche CNIL.

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
2	Authentification des utilisateurs *(suite)*	– **Plus de 5 caractères** si l'authentification comprend une information complémentaire. L'information complémentaire doit utiliser **un identifiant confidentiel d'au moins 7 caractères** et bloquer le compte à la 5e tentative infructueuse. – Le mot de passe peut ne faire que **4 caractères** si l'authentification s'appuie sur un matériel détenu par la personne et si le mot de passe n'est utilisé que pour déverrouiller le dispositif matériel détenu en propre par la personne (par exemple une carte à puce ou téléphone portable) et qui se bloque à la 3e tentative infructueuse. – **Obliger l'utilisateur à changer son mot de passe après réinitialisation.** – **Limiter le nombre de tentatives d'accès à un compte.**	
3	Gestion des habilitations. (Limiter les accès aux seules données dont un utilisateur a besoin)	• **Définir des profils d'habilitation** dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions. • **Supprimer les permissions d'accès** des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat. • **Réaliser une revue annuelle des habilitations** afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.	
4	Traçage des accès et gestion des incidents. (Journalisation des accès et mise en place de procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).	• **Prévoir un système de journalisation** (enregistrement dans des « fichiers journaux » ou *« logs »*) des activités des utilisateurs, des anomalies et des événements liés à la sécurité : – Ces journaux doivent conserver les événements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important). – **La journalisation doit concerner, au minimum, les accès des utilisateurs** en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion. – Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné.	

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
4	Traçage des accès et gestion des incidents. *(suite)*	• **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des représentants du personnel. • **Protéger les équipements de journalisation et les informations journalisées** contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée. • Établir des procédures détaillant la surveillance de l'utilisation du traitement et **examiner périodiquement les journaux d'événements** pour y détecter d'éventuelles anomalies. • S'assurer que les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable du traitement. • **Prévoir des procédures pour les notifications de violation de données à caractère personnel et notifier à la CNIL ainsi qu'aux personnes concernées**, sauf exception prévue par le RGPD, pour qu'elles puissent en limiter les conséquences.	
5	Sécurisation des postes de travail (Prévenir les accès frauduleux, l'exécution de virus ou la prise de contrôle à distance, notamment *via* Internet)	• Prévoir un mécanisme de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné. • Installer un **« pare-feu »** (*« firewall »*) logiciel, et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail. • Utiliser des **antivirus régulièrement mis à jour** et prévoir une politique de **mise à jour régulière des logiciels**. • Configurer les logiciels pour que les **mises à jour de sécurité se fassent automatiquement** dès que cela est possible. • **Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme** plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation. • **Limiter la connexion de supports mobiles** (clés USB, disques durs externes, etc.) à l'indispensable. • Désactiver l'exécution automatique (*« autorun »*) depuis des supports amovibles. • Pour l'assistance sur les postes de travail : recueillir l'**accord de l'utilisateur avant toute intervention sur son poste.**	

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
6	Sécurisation de l'informatique mobile (Anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile)	• **Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles** (ex : vol de matériel) et aux procédures prévues pour les limiter. • **Mettre en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation** des postes nomades, pour se prémunir contre la disparition des données stockées. Prévoir **des moyens de chiffrement des postes nomades et supports de stockage mobiles** (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.), par exemple : – le chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose ; – le chiffrement fichier par fichier ; – la création de conteneurs (fichier susceptible de contenir plusieurs fichiers) chiffrés. De nombreux ordinateurs portables intègrent une solution de chiffrement du disque dur : le cas échéant, il convient d'utiliser cette fonctionnalité. • **Concernant les *smartphones***, en plus du code PIN de la carte SIM, **activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller** (mot de passe, schéma, etc.).	
7	Protection du réseau informatique interne	• **Limiter les accès Internet** en bloquant les services non nécessaires (VoIP, pair à pair, etc.). • **Gérer les réseaux Wi-Fi :** utiliser un chiffrement conforme à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et s'assurer que les réseaux ouverts aux invités sont séparés du réseau interne. • **Imposer un VPN pour l'accès à distance** ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boîtier générateur de mots de passe à usage unique (OTP), etc.). • **S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet.** La télémaintenance doit s'effectuer à travers un VPN. • **Limiter les flux réseau au strict nécessaire** en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.	

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
8	Sécurisation des serveurs. (Renforcer les mesures de sécurité appliquées aux serveurs)	• **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.** • Utiliser des comptes de moindres privilèges pour les opérations courantes. • **Adopter une politique spécifique de mots de passe** pour les administrateurs. Changer les mots de passe, au moins, lors de chaque départ d'un administrateur et en cas de suspicion de compromission. • **Installer les mises à jour critiques** sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire. • En matière **d'administration de bases de données :** – **Utiliser des comptes nominatifs** pour l'accès aux bases de données et créer des comptes spécifiques à chaque application. – Mettre en œuvre des mesures contre les attaques par injection de code SQL, de scripts, etc. • **Effectuer des sauvegardes et les vérifier régulièrement.** • **Assurer une disponibilité des données.** • **Mettre en œuvre le protocole TLS**[212] (en remplacement de SSL), ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout change de données sur internet et vérifier sa bonne mise en œuvre par des outils appropriés. (Pour le protocole TLS, il existe par exemple : https://www.ssllabs.com/ssltest/ ou https://ssl-tools.net/).	
9	Sécurisation des sites web	• **Mettre en œuvre le protocole TLS**[213] (en remplacement de SSL) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre. • **Rendre l'utilisation de TLS obligatoire** pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.	

[212] Le protocole TLS est parfois appelé SSL ou SSL/TLS, « SSL » étant le nom donné à ce protocole pour ses premières versions considérées aujourd'hui comme vulnérables et à éviter.
[213] *Ibid.*

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
9	Sécurisation des sites web	• **Limiter les ports de communication** strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports. • **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.** En particulier, limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent. • **Recueil du consentement aux cookies utilisés non nécessaires au service**, après information de l'internaute et avant le dépôt du *cookie*. • **Limiter le nombre de composants mis en œuvre**, en effectuer une veille et les mettre à jour. • **Vérifier qu'aucun mot de passe ou identifiant ne passe dans les URL.** • **Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu.**	
10	Continuité d'activité et sauvegardes (Effectuer des sauvegardes régulières pour limiter l'impact d'une disparition non désirée de données)	• **S'agissant de la sauvegarde des données :** – **Effectuer des sauvegardes fréquentes des données**, que celles-ci soient sous forme papier ou électronique. Il peut être opportun de prévoir des sauvegardes incrémentales quotidiennes et des sauvegardes omplètes à intervalles réguliers. – **Stocker les sauvegardes sur un site extérieur, dans un endroit sûr**, si possible dans des coffres ignifugés et étanches. – **Prévoir des moyens de sécurité pour le convoyage des sauvegardes.** – **Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation** (par exemple les sauvegardes, en prévoyant un stockage dans un lieu sécurisé, en encadrant contractuellement une prestation d'externalisation des sauvegardes). – Lorsque les sauvegardes sont transmises par le réseau, il convient de chiffrer le canal de transmission si celui-ci n'est pas interne à l'organisme.	

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
10	Continuité d'activité et sauvegardes *(suite)*	• **S'agissant de la reprise et de la continuité d'activité.** – **Rédiger un plan de reprise et de continuité d'activité informatique** même sommaire, incluant la liste des intervenants. – S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident. – **Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.** – À propos des matériels : utiliser un onduleur pour protéger le matériel servant aux traitements essentiels et prévoir une redondance matérielle des matériels de stockage, par exemple au moyen d'une technologie RAID.	
11	Archivage sécurisé[214]	• **Définir un processus de gestion des archives :** quelles données doivent être archivées, comment et où sont-elles stockées, comment sont gérées les données descriptives ? • **Mettre en œuvre des modalités d'accès spécifiques aux données archivées** du fait que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle. • **Détruire les archives obsolètes de manière sécurisée, et notamment choisir un mode opératoire garantissant que l'intégralité d'une archive a été détruite.**	
12	Encadrement de la maintenance et de la destruction des données[215]	• **Enregistrer les interventions de maintenance dans une main courante.** • **Insérer une clause de sécurité dans les contrats de maintenance effectuée par des prestataires.** • Encadrer par un responsable de l'organisme les interventions par des tiers. • **Rédiger et mettre en œuvre une procédure de suppression sécurisée des données.** • **Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin du contrat de location.**	

[214] Les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation doivent être archivées de manière sécurisée (par exemple : les données conservées afin d'être utilisées en cas de contentieux).
[215] Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels.

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
13	Gestion de la sous-traitance (Encadrer la sécurité des données avec les sous-traitants)	• **Faire appel uniquement à des sous-traitants présentant des garanties suffisantes**[216] (notamment en termes de connaissances spécialisées, de fiabilité et de ressources). Exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information. • **Prendre et documenter les moyens (audits de sécurité, visite des installations, etc.)** permettant d'**assurer l'effectivité des garanties offertes par le sous-traitant** en matière de protection des données. Ces garanties incluent notamment : – Le chiffrement des données selon leur sensibilité ou à défaut des procédures garantissant que la société de prestation n'a pas accès aux données si cela n'est pas nécessaire. – Le chiffrement des transmissions de données (ex. : connexion de type HTTPS, VPN, etc.). – Des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc. • **Prévoir un contrat avec les sous-traitants**, prévoyant notamment l'objet, la durée, la finalité du traitement et les obligations des parties et en particulier des dispositions fixant : – Leur obligation en matière de **confidentialité des données personnelles** confiées. – Des **contraintes minimales en matière d'authentification** des utilisateurs. – **Les conditions de restitution et/ou de destruction des données** en fin du contrat. – **Les règles de gestion et de notification des incidents** (information du RT dans les plus brefs délais en cas de faille/incident de sécurité ou de violation de données personnelles).	

[216] Cf. Fiche 10 du guide *« Gestion de la sous-traitance »*

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
14	Sécurisation des échanges avec d'autres organismes. (Renforcer la sécurité de toute transmission de données à caractère personnel)	• **Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers** (DVD, clé USB, disque dur portable). • Lors d'un envoi *via* un réseau : – **Chiffrer les pièces** sensibles à transmettre, si cette transmission utilise la messagerie électronique (voir point 17). – Utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple **SFTP** ou **HTTPS**, en utilisant l**es versions les plus récentes des protocoles.** – **Assurer la confidentialité des secrets** (clé de chiffrement, mot de passe, etc.) en les transmettant *via* un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS). • **S'assurer de l'identité du destinataire.**	
15	Protection des locaux (Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux)	• Installer des **alarmes anti-intrusion** et les vérifier périodiquement. • **Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies**, et les inspecter annuellement. • Protéger les clés permettant l'accès aux locaux et les codes d'alarme. • **Distinguer les zones des bâtiments selon les risques** (par exemple prévoir un contrôle d'accès dédié pour la salle informatique). • Tenir à jour une liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone. • **Restreindre les accès aux locaux au moyen de portes verrouillées.** • **Établir les règles et moyens de contrôle d'accès** des visiteurs, au minimum en faisant **accompagner les visiteurs, en dehors des zones d'accueil du public** par une personne appartenant à l'organisme. • Protéger physiquement les Protéger physiquement les matériels informatiques par des moyens spécifiques (système anti-incendie dédié, surélévation contre les inondations, redondance d'alimentation électrique et/ou de climatisation, etc.).	

	Mesures de sécurités techniques et organisationnelles	Résumé des mesures *(À adapter sur la base des mesures de sécurité élémentaires préconisées par la CNIL et reprises ci-dessous pour information)*	Documents de référence – Date [210]
16	Encadrement des développements informatiques (Intégrer sécurité et protection de la vie privée au plus tôt dans les projets)	• **Intégrer la protection de la vie privée et la sécurité des données, dès la conception** de l'application ou du service. Ces exigences peuvent se traduire par des choix d'architecture (décentralisée vs. centralisée), de fonctionnalités (anonymisation à bref délai, minimisation des données), de technologies (chiffrement des communications), etc. • **Pour tout développement à destination du grand public, mener une réflexion sur les paramètres relatifs à la vie privée**, et notamment sur le paramétrage par défaut. • Éviter le recours à des zones de texte libre ou de commentaires ou les encadrer strictement. • **Effectuer les développements informatiques et les tests** dans un environnement informatique distinct de celui de la production (par exemple, sur des ordinateurs ou des machines virtuelles différents) et **sur des données fictives ou anonymisées.**	
17	Chiffrage des données (Assurer l'intégrité, la confidentialité et l'authenticité d'une information)	• **Utiliser un algorithme reconnu et sûr pour**, par exemple : – Hacher les données : SHA-256, SHA-512, SHA-3. – Stocker les mots de passe : HMAC utilisant SHA-256, bcrypt, scrypt ou PBKDF2. – Le chiffrement symétrique : AES ou AES-CBC. – Le chiffrement asymétrique : RSA-OAEP comme défini dans PKCS#1 v2.1. – Les signatures : RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1. • **Utiliser les tailles de clés suffisantes pour AES** il est recommandé d'utiliser des clés de 128 bits et, pour les algorithmes basés sur RSA, des modules et exposants secrets d'au moins 2 048 bits ou 3072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65536. • **Conserver les clés secrètes et cryptographiques de manière sécurisée,** au minimum par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr. • **Prévoir une procédure relative à la gestion des clés et certificats** en prenant en compte les cas d'oubli de mot de passe de déverrouillage.	

Contrôle et sanctions de la CNIL

Contrôle et sanctions de la CNIL

Fiche n° 9

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

En tant qu'autorité administrative indépendante, la CNIL dispose du pouvoir de contrôler la conformité de tout organisme situé sur le territoire français mettant en œuvre des traitements de données à caractère personnel dans le cadre de ses activités, que le traitement ait lieu en France ou hors de France[217].

Lors d'un contrôle, la CNIL s'intéresse notamment à la finalité du traitement, à sa base légale, à la nature des données traitées, aux modalités d'information des personnes concernées, aux durées de conservation des données, aux destinataires des données, aux mesures de sécurité mises en œuvre et aux transferts internationaux de données personnelles[218].

La CNIL peut effectuer quatre types de contrôles, qui peuvent se cumuler entre eux :

- Le contrôle **sur place** (visite des agents dans les locaux d'un responsable du traitement ou d'un sous-traitant).
- Le contrôle **sur pièces** (envoi d'un questionnaire destiné à évaluer la conformité des traitements mis en œuvre par le responsable du traitement ou le sous-traitant).
- Le contrôle **sur audition** (convocation par les agents de la CNIL de toute personne susceptible de leur fournir des renseignements ou informations utiles à l'accomplissement de leur mission)[219].
- Le contrôle **en ligne** (consultation par les agents de la CNIL depuis ses locaux de toutes données librement accessibles ou rendues librement accessibles y compris par imprudence, négligence ou du fait d'un tiers).

La présente fiche se concentrera principalement sur les opérations de **contrôle sur place** (Il est néanmoins préconisé à chaque cabinet de formaliser en interne ce qu'il convient de faire dans les autres cas de contrôle, en particulier dans le cadre du contrôle sur pièces et/ou en ligne).

Dans le cadre d'un contrôle, les agents de la CNIL sont habilités à avoir accès à tout document ou système informatique utile à leurs opérations de contrôle, dans le respect du secret professionnel du commissaire aux comptes. Par ailleurs, les agents peuvent également s'entretenir avec le personnel de votre cabinet et prendre connaissance des procédures mises en place.

Le refus de communiquer aux agents de la CNIL les renseignements ou documents utiles à leur mission est susceptible de constituer le délit d'entrave[220]. A la fin des opérations de contrôle sur place, les agents dressent un procès-verbal auquel vous pouvez apporter des observations.

[217] Article 8 g) de la Loi informatique et libertés du 7 janvier 1978.
[218] Charte des contrôles de la CNIL en date du 05 août 2020
[219] Article 34 du décret n° 2019-536 du 29 mai 2019 : *« Les agents habilités peuvent entendre toute personne susceptible de leur fournir tout renseignement ou toute justification utile pour l'accomplissement de leur mission. Les agents habilités adressent la convocation par lettre remise contre signature ou remise en main propre contre récépissé ou acte d'huissier ».*
[220] Article 226-22-2 du Code pénal : *« Est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés (…) en refusant de communiquer à ses membres ou aux agents habilités (…) les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ».*

Le suivi rigoureux post contrôle avec la CNIL et la mise en œuvre de mesures correctives (si nécessaires) de manière proactive sont fortement recommandés.

À l'issue de l'instruction du dossier, la CNIL établit un rapport qui peut donner lieu à la clôture du dossier (lorsqu'aucun manquement significatif n'est relevé), une lettre d'observations ou de mise en demeure, publique ou non, qui pourra servir de base à une éventuelle procédure de sanction.

En cas de manquement à la Règlementation applicable en matière de protection des données personnelles, la CNIL peut prendre diverses sanctions, pouvant être rendues publiques, allant de l'injonction à une amende administrative d'un montant maximal de 4 % du chiffre d'affaires annuel mondial ou de 20 millions d'euros.

Contrôle et sanctions de la CNIL

Sommaire

1. Quelles sont les causes d'un contrôle ?

L'autorité de contrôle peut décider d'effectuer un contrôle :

- **À la suite d'une plainte, d'une réclamation ou d'une pétition émanant de personnes concernées :** Traditionnellement, les contrôles interviennent à la suite d'une plainte d'une personne concernée. Il peut ainsi s'agir d'un ancien salarié, d'un candidat à l'embauche, d'un client mécontent de la manière dont ses données personnelles ont été traitées, etc.[221].
- Selon la nature et la gravité des faits signalés à la CNIL, celle-ci peut décider du déclenchement d'une opération de contrôle. Aussi, de manière à éviter les plaintes, il est recommandé de respecter les délais de réponse aux demandes d'exercice de droits des personnes concernées (avec si besoin un accusé de réception promettant une réponse dans un délai court, si la réponse complète n'est pas possible dans les délais) et lorsque vous n'êtes pas en mesure d'y répondre favorablement, d'informer les personnes concernées et de motiver votre réponse.
- **En réaction à un sujet d'actualité :** Les contrôles peuvent également être liés à des sujets d'actualité (Covid-19 par exemple).
- **Dans le cadre de son programme annuel de contrôles :** La CNIL publie chaque année son programme d'action et sa stratégie de contrôle[222].
- **En réaction à une violation de données personnelles au sein de l'organisme :** La CNIL peut décider de contrôler un organisme qui vient de subir une violation de données à caractère personnel (fuite de données, faille de sécurité…).
- **Après une mise en demeure :** La CNIL peut décider d'effectuer un contrôle afin de vérifier si sa première mise en demeure a été prise en compte par l'organisme.
- **À la demande d'une autre autorité de contrôle de l'UE ou dans le cadre d'une démarche conjointe.**

2. Le contrôle sur place : L'arrivée des agents dans les locaux

Dans le cadre d'un contrôle sur place, les agents de la CNIL se rendent directement dans les locaux de l'organisme contrôlé, auxquels ils ont accès de 6 heures à 21 heures[223].

Dès lors que le contrôle a débuté dans cet intervalle, les agents peuvent prolonger le contrôle au-delà de 21 heures si nécessaire. Les entreprises contrôlées sont très rarement prévenues

[221] La CNIL estime que les plaintes et réclamations sont à l'origine de plus de 40 % de ses contrôles.
[222] À titre d'exemple, la CNIL a annoncé trois thématiques de contrôle prioritaires pour l'année 2021 – la sécurité des données de santé, la cyber sécurité du web français et le respect des règles applicables aux cookies et autres traceurs – censés représenter au moins 20 % des procédures formelles de contrôle menées par la CNIL.
[223] Article 19 de la Loi informatique et liberté du 7 janvier 1978 : *« Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités (…) ont accès, **de 6 heures à 21 heures**, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel ».*

à l'avance. La délibération autorisant le contrôle sur place est généralement notifiée le jour de l'arrivée des agents sur les lieux[224].

La délégation est généralement composée de deux agents, un juriste et un auditeur des systèmes d'information, ayant respectivement des compétences juridiques et techniques.

• Ce qu'il faut faire :

✓ Identifier en amont, les coordonnées d'un ou plusieurs cabinets d'avocats spécialisés à contacter en cas d'urgence ou de contrôle CNIL.

✓ Identifier qui au sein de votre structure peut être habilité à recevoir des agents de la CNIL (notamment en cas d'absence de l'associé en charge au moment du contrôle).

✓ Informer sans délai votre DPO (si désigné), les organes dirigeants, le responsable informatique/DSI et plus généralement tout responsable dont la présence peut être utile.

✓ Vérifier, à titre de précaution, la carte professionnelle des agents de la CNIL qui se présentent à vous ainsi que, le cas échéant, leur habilitation (sans en conserver de copie)[225].

✓ Lire **l'ordre de mission** des agents de la CNIL se présentant (il s'agit de l'ordre spécifiant l'objet du contrôle et sa portée, en général il s'agit d'une délibération signée par la Présidente de la CNIL).

✓ Mettre une salle de réunion à la disposition des agents pour qu'ils puissent s'installer.

✓ Contacter votre avocat spécialisé sur ces questions (si vous l'estimez nécessaire). Votre avocat pourra vous assister durant le contrôle et vous guider au mieux dans les réponses et documents à fournir[226]. La CNIL ne peut pas s'opposer à ce que vous soyez assisté par votre avocat. Pour autant, le contrôle n'est pas suspendu jusqu'à l'arrivée de celui-ci sur place.

✓ Ne répondre qu'aux questions posées, et ne pas communiquer plus de documents que ceux demandés.

✓ Prendre note des éléments et informations relatifs au contrôle (personnes interrogées, documents consultés par les agents, questions posées, etc.).

✓ En tout état de cause (et quel que soit le type de contrôle), répondre dans les temps aux agents de la CNIL et ne pas faire obstruction à leur mission (communiquer les pièces demandées dans un délai raisonnable et dans un format facilement exploitable, à déterminer avec les agents).

Pour rappel : l'article 31 du RGPD dispose que le responsable du traitement, le sous-traitant et leur représentant coopèrent avec l'autorité de contrôle à la demande de celle-ci dans l'exécution de ses missions.

[224] Article 26 du décret 2019-536 du 29 mai 2019 : *« Lorsque la commission effectue un contrôle sur place, elle informe **au plus tard lors de son arrivée sur place** le responsable des lieux ».*

[225] Seuls les agents titulaires d'une habilitation de la CNIL peuvent effectuer des contrôles et vérifications. La liste des agents habilités est publiée dans une délibération de la CNIL accessible en ligne.

[226] L'organisme faisant l'objet d'un contrôle sur place ou sur audition a le droit de se faire assister d'un conseil, avocat ou expert privé de son choix ou à défaut, de deux témoins (qui ne sont pas placés sous l'autorité des agents de la CNIL).

• **Ce qu'il ne faut pas faire :**

- ⊘ Donner accès à ses locaux à n'importe quel(s) individu(s) se présentant comme des agents de la CNIL sans vérification préalable (risque de fraude).
- ⊘ Faire usage de son droit d'opposition à des fins purement dilatoires ou sans motif impérieux valable.
- ⊘ Faire obstruction aux agents de la CNIL en refusant de communiquer des documents, des données (cf. délit d'entrave).
- ⊘ Laisser les agents de la CNIL dans les locaux sans aucun accompagnement.

2.1 Peut-on s'opposer au contrôle sur place ?

En vertu de la loi informatique et libertés, vous disposez en principe d'un droit d'opposition à la visite[227]. Cependant, il est déconseillé de l'exercer sans motif réellement valable.

Si vous exercez votre droit d'opposition, les agents de la CNIL portent au procès-verbal les motifs de votre opposition et saisissent le juge des libertés et de la détention du Tribunal judiciaire territorialement compétent afin que ce dernier autorise dans un délai de 48 heures la poursuite des opérations.

> *À noter :* le fait de s'opposer au contrôle de la CNIL alors que la visite a été autorisée par le juge des libertés et de la détention ou le refus de communiquer aux agents de la CNIL les renseignements ou documents utiles à leur mission est susceptible de constituer un délit d'entrave puni d'un an d'emprisonnement et de 15 000 euros d'amende (montant porté au quintuple pour les personnes morales)[228] conformément aux dispositions de l'article 226-22-2 du Code pénal.

2.2 Le déroulement du contrôle sur place

Dans le cadre de leurs opérations de contrôle, les agents de la CNIL *« peuvent **demander communication de tous documents** nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie »*[229].

Par exemple : les agents de la CNIL peuvent vous demander de leur communiquer une copie des contrats de sous-traitance informatique, des formulaires de collecte, votre registre des traitements, etc.

Les agents de la CNIL peuvent également avoir accès aux programmes informatiques, aux ordinateurs professionnels, et aux données utiles à leur mission et en prendre une copie sécurisée[230].

[227] Article 19-II de la Loi informatique et libertés du 6 janvier 1978 : *« Le responsable de ces lieux, locaux, enceintes, installations ou établissements est informé de son droit d'opposition à la visite ».*
[228] Article 131-38 du Code pénal : *« le taux maximum de l'amende applicable aux personnes morales est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ».*
[229] Article 19-III. al.1 de la Loi informatique et libertés du 6 janvier 1978.
[230] Article 19-III de la Loi informatique et libertés du 6 janvier 1978 : *« Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, **aux programmes informatiques et aux données** ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle ».*

Par exemple : les agents de la CNIL peuvent vous demander de leur donner accès à votre outil de CRM pour vérifier notamment les zones de commentaires libres, les durées de conservation, etc.

Les agents de la CNIL peuvent demander à s'entretenir avec tout membre du personnel susceptible de détenir des informations utiles à leur mission. Si le membre en question n'est pas disponible sur place ou par téléphone, vous pouvez réserver la réponse.

Par exemple : les agents de la CNIL peuvent demander à s'entretenir avec le DSI de votre cabinet pour prendre connaissance des mesures de sécurité mises en place.

Enfin, les agents de la CNIL peuvent effectuer des vérifications auprès de vos sous-traitants (hébergeur, maintenance…).

À noter : les agents de la CNIL sont soumis au secret concernant les faits, actes ou renseignements dont ils ont connaissance dans le cadre de leurs missions[231]. Il n'est donc pas possible d'exiger d'eux qu'ils signent un accord de confidentialité. Il est néanmoins toujours utile d'être présent lors de la remise de certains documents et d'opérer la remise sous contrôle de votre conseil habituel.

Il est recommandé de conserver une copie des éléments remis aux agents de la CNIL dans le cadre du contrôle. Le procès-verbal de contrôle (dont une copie est communiquée à l'organisme contrôlé) énumère l'ensemble des pièces communiquées.

Enfin, il est important de se faire préciser le périmètre du contrôle par les agents de la CNIL, notamment lorsqu'il y a plusieurs entités à une même adresse (experts comptables, cabinets d'avocats, par exemple.)

Les agents de la CNIL peuvent-ils exiger la communication des correspondances entre le commissaire aux comptes et son avocat ?

Non, la CNIL ne peut exiger la communication des échanges entre le commissaire aux comptes et son avocat. Le commissaire aux comptes peut néanmoins décider de les communiquer (ou seulement une partie) s'il le juge opportun, notamment pour montrer aux agents de la CNIL les travaux juridiques effectués/en cours concernant sa conformité à la Règlementation applicable.

À la fin des opérations de contrôle, les agents rédigent un procès-verbal de fin de contrôle qui précise[232] :

- La nature, le jour, l'heure et le lieu des vérifications effectuées.
- L'objet de la mission, les membres présents, les personnes rencontrées et leurs éventuelles déclarations, les demandes formulées par les membres de la mission et les éventuelles difficultés rencontrées.

[231] Article 20 de la Loi informatique et libertés du 6 janvier 1978 : *« Les agents de la commission sont astreints au secret pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions ».*
[232] Article 19 de la Loi informatique et liberté du 6 janvier 1978 : *« Il est dressé procès-verbal des vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation ».*

– Les pièces qui lui ont été remises et la liste des informations, pièces ou actions complémentaires à fournir ou réaliser dans un délai déterminé (des copies sont annexées au procès-verbal).

À noter : Dans le cadre des contrôles sur place et sur audition, le procès-verbal est établi contradictoirement. Il convient d'en prendre connaissance avant de le signer car vous pouvez demander à y faire figurer vos commentaires et plus généralement toute difficulté rencontrée lors du contrôle. Il est généralement préférable de faire mentionner quelques réserves d'usage et de relire attentivement le procès-verbal afin de corriger toute erreur et apporter toute précision ou réserve utile si le procès-verbal ne reflète pas le déroulement de la visite ou les réponses qui ont été apportées.

Exemple de réserve : *« Ces informations ont été communiquées en l'état de notre connaissance du **<Système X>**, sachant que **M. X**, n'a pu être joint pendant le contrôle. Nous nous réservons le droit d'apporter des précisions et corrections complémentaires ultérieurement, après avoir pris attache avec **M. X** ».*

Le procès-verbal est signé par les agents de la CNIL et le représentant de l'entité contrôlée. En cas de refus ou d'absence de signature, une mention en est portée au procès-verbal. Le procès-verbal est ensuite notifié à l'organisme ayant fait l'objet du contrôle dans un délai de 15 jours par courrier recommandé avec accusé de réception.

Faut-il informer les entités (clientes du commissaire aux comptes) du contrôle opéré notamment si les agents de la CNIL ont eu accès à certains documents ou certaines informations ?

En principe, cela n'est pas nécessaire mais il est préférable de demander conseil à votre avocat.

Les agents de la CNIL peuvent-ils avoir accès à un dossier client et en prendre copie dans le cadre du contrôle ?

En vertu de l'article L. 822-15 du Code de commerce, les commissaires aux comptes ne peuvent être déliés de leur secret professionnel que par une disposition législative particulière expresse[233]. En l'absence d'une telle disposition, ils doivent opposer leur secret professionnel aux agents de la CNIL.

En conséquence, le dossier de travail ne peut être remis aux contrôleurs.

En tout état de cause, la Charte des contrôles de la CNIL rappelle que les agents de la CNIL sont tenus au respect des principes de proportionnalité et de minimisation des données[234] et que seuls les agents ayant besoin d'en connaître peuvent accéder au dossier de contrôle. (Pour plus d'informations, consultez la Charte des contrôles de la CNIL, rubrique *« Quelles sont les obligations des agents de contrôle de la CNIL ? »*).

[233] Article L. 822-15 du Code de commerce : *« Sous réserve des dispositions de l'article L. 823-12 et des dispositions législatives particulières, les commissaires aux comptes, ainsi que leurs collaborateurs et experts, sont astreints au secret professionnel pour les faits, actes et renseignements dont ils ont pu avoir connaissance à raison de leurs fonctions ».*

[234] Charte des contrôles de la CNIL : *« Les pièces collectées doivent servir strictement aux fins de l'objet de la mission décidé par la Présidente de la CNIL et porté dans la décision de contrôle. Les contrôleurs veillent à minimiser les données collectées en contrôle, que celles-ci soient des données personnelles ou non ».*

3. Le suivi post-contrôle

Dans la majorité des cas, les opérations de contrôle font apparaître au sein de l'organisme contrôlé des points à améliorer et corriger dans le traitement des données personnelles.

Vous pouvez également être amené à l'issue d'une opération de contrôle ou d'une procédure de sanction à rester en contact avec les agents de la CNIL afin de les tenir informés des mesures correctives mises en place.

Il est donc important d'assurer un suivi post-contrôle et de respecter les échéances qui vous sont fixées (ou de demander un délai supplémentaire pour des raisons motivées).

> *À noter :* Postérieurement au contrôle et pendant toute la période d'instruction du dossier, vous disposez du droit de faire des observations complémentaires. Il est recommandé de tenir la CNIL informée de la mise en œuvre des actions correctrices que vous mettez en place.

Les agents consignent au dossier d'instruction les courriers, e-mails et les pièces communiquées par l'organisme faisant l'objet du contrôle aux agents post-contrôle. Le dossier de contrôle est stocké de manière sécurisée et est conservé pendant toute la durée de la procédure puis détruit cinq ans après la clôture de la procédure (sauf exercice des voies de recours).

La décision rendue tient donc compte de l'ensemble des échanges intervenus (y inclus des actions correctrices réalisées).

- **Les bonnes pratiques :**

✓ Définir un ou plusieurs interlocuteurs au sein de votre structure pour échanger avec la CNIL et suivre la bonne mise en place des mesures.

✓ Ne pas attendre que la CNIL notifie les actions correctrices à opérer si celles-ci sont identifiées ou identifiables : soyez proactifs et tenez les agents informés des mesures mises en place (par exemple : mise à jour de la politique de confidentialité des données, ou du registre des traitements si celui-ci était incomplet).

4. Le rapport établi par la CNIL

À la suite des opérations de contrôle, la CNIL prend connaissance de manière plus précise des documents dont elle a pris copie lors des opérations de contrôle et réalise un rapport. Les échanges avec la CNIL en réponse à des questions complémentaires peuvent durer plusieurs mois.

Ce rapport est notifié à l'organisme ayant fait l'objet du contrôle qui peut déposer des observations orales devant la formation restreinte qui statuera sur une éventuelle sanction, si des manquements sont constatés. Ce rapport a vocation à servir de base à une éventuelle procédure de sanction[235].

[235] Article 22 de la Loi informatique et libertés du 6 janvier 1978 : *« Les mesures prévues au III de l'article 20 et aux 1° à 7° du I de l'article 21 de la présente loi sont prononcées* ***sur la base d'un rapport*** *établi par l'un des membres de la Commission nationale de l'informatique et des libertés ».*

5. La procédure de sanction en cas de manquement

Un contrôle peut avoir différentes issues possibles :

- **En l'absence de manquement ou en présence de manquements peu significatifs**, la procédure est clôturée par un courrier du Président de la CNIL accompagné d'observations (ex. : modifier les mentions d'informations, supprimer des données obsolètes, etc.).
- **En présence de manquements plus significatifs**, du Président de la CNIL peut saisir la formation restreinte de la CNIL afin qu'une sanction soit prononcée ou que l'organisme contrôlé soit mis en demeure[236] d'adopter des mesures correctrices dans un délai imparti. Cette mise en demeure est généralement rendue publique afin d'inciter l'organisme à s'y conformer.

> *À noter :* en cas d'absence de réponse à la lettre de mise en demeure ou de non-respect de ses injonctions, le Président de la CNIL peut transmettre le dossier à la formation restreinte compétente pour prononcer une sanction et/ou transmettre le dossier au Parquet en vue de poursuites judiciaires.

La formation restreinte de la CNIL peut prononcer différents types de sanctions :

- L'injonction, y compris sous astreinte, de se mettre en conformité.
- La limitation temporaire ou définitive du traitement.
- L'interdiction du traitement.
- Le retrait d'une autorisation accordée.
- La suspension des flux de données vers un destinataire situé dans un pays tiers ou une organisation internationale.
- Une amende administrative pouvant s'élever, selon les cas, à la somme la plus élevée entre 4 % du chiffre d'affaires mondial ou 20 000 000 euros[237].

Les sanctions prononcées par la CNIL sont généralement rendues publiques sur le site de la CNIL et de Légifrance. Pour plus d'informations, vous pouvez vous référer à la fiche de la CNIL sur la procédure de sanction.

> *À noter :* les décisions de la CNIL peuvent faire l'objet de recours devant le Conseil d'État (recours de plein contentieux, référé-suspension ou référé-liberté selon les cas).

[236] Charte des contrôles de la CNIL : *« La mise en demeure est une décision de la Présidente de la CNIL qui énumère les manquements reprochés à l'organisme ainsi que les mesures qu'il doit prendre pour se mettre en conformité. Le délai imparti pour se mettre en conformité varie entre 24 heures (en cas d'extrême urgence) et 6 mois (…). La Présidente de la CNIL peut décider de faire procéder à des vérifications après la mise en demeure afin de s'assurer de la mise en conformité de l'organisme ».*

[237] Article 83 du RGPD.

Exemples de sanctions récentes (Pour plus d'exemples de décisions de sanction, vous pouvez consulter la page « Sanctions » du site de la CNIL)

Décision	Manquement(s) reproché(s)	Sanction(s)
Délibération n° MED 2019-035 du 31 décembre 2019 et n° MEDP 2020_001 du 20 janvier 2020	• Non-respect des règles relatives au recueil du consentement (rédaction de la mention accompagnant la case à cocher susceptible d'induire en erreur l'abonné sur la portée de son engagement, impossibilité pour l'utilisateur de donner son consentement par finalité de manière spécifique). • Durée de conservation excessive des données en base active au regard des finalités poursuivies (en l'espèce, 5 ans au lieu de la durée de 14 mois prévue par le Code de la consommation).	Mise en demeure rendue publique[238], sous 3 mois de : ➪ Recueillir un consentement libre spécifique, éclairé et univoque des utilisateurs. ➪ Mettre en place une politique de durée de conservation des données.
Délibération n° SAN du 21 novembre 2019	• Manquement aux règles de démarchage téléphonique. • Absence de mécanisme centralisé permettant la prise en compte des demandes d'opposition exprimées par les personnes démarchées. • Présence de commentaires injurieux dans les zones de commentaire libres du logiciel de gestion des clients. • Manquement à l'obligation d'information des personnes concernées. • Manquement à l'obligation de coopérer avec l'autorité de contrôle.	500 000 euros d'amende. Injonction de mise en conformité sous astreinte de 500 euros par jour de retard. Publication de la décision pour une durée de 2 ans.
Délibération n° SAN 2019-007 du 18 juillet 2019	• Manquements à l'obligation de sécurité des données : robustesse insuffisante des mots de passe de connexion à l'espace personnel des clients en ligne, transmission des mots de passe en clair dans un courriel non chiffré, défectuosité du site web, absence de mesures élémentaires de sécurité rendant accessibles les données des clients par une simple modification de l'url.	180 000 euros d'amende. Publication de la décision pour une durée de 2 ans.
Délibération n° SAN 2019-001 du 21 janvier 2019	• Manquement aux obligations de transparence et d'information (défaut global d'accessibilité de l'information, non-respect des exigences de clarté et de compréhension de l'information excessivement éparpillée dans plusieurs documents, description imprécise et incomplète des données collectées et des finalités poursuivies). • Manquement à l'obligation de disposer d'une base légale pour les traitements mis en œuvre (non-respect des règles relatives au recueil d'un consentement éclairé et univoque).	50 000 000 d'euros d'amende. Publication de la décision pendant une durée de 2 ans.

[238] Dans sa délibération, la CNIL rappelle que *« cette mise en demeure ne revêt pas le caractère d'une sanction. À ce titre, aucune suite ne sera donnée à la procédure si l'organisme concerné se conforme en tout point aux exigences de la mise en demeure dans le délai imparti »*.

Gestion de la sous-traitance

Gestion de la sous-traitance

Fiche n° 10

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Synthèse

Cette fiche a pour objet de vous guider dans la gestion des relations contractuelles avec vos sous-traitants au sens du RGPD, c'est-à-dire aux personnes physiques ou morales qui traitent pour votre compte les données à caractère personnel que vous leur confiez[239].

La présente fiche n'a pas vocation à s'appliquer aux relations avec des prestataires/fournisseurs qui ne traitent aucune donnée personnelle ou encore à ceux qui sont responsables de traitements[240].

Comme toute entreprise, vous êtes amené à faire appel à des prestataires/fournisseurs. Pour autant, tous ces tiers ne sont pas nécessairement des « sous-traitants au sens du RGPD ».

En faisant appel à des prestataires/fournisseurs tiers, vous devez :

1. Vérifier si les fournisseurs/prestataires en question sont amenés à traiter[241] des données à caractère personnel.
2. Si oui, déterminer si ces tiers agissent selon vos instructions et pour votre compte (auquel cas ils sont vos sous-traitants au sens du RGPD).
3. Identifier les catégories de données auxquelles vos sous-traitants (au sens RGPD) ont accès.
4. Localiser leurs activités de traitements afin d'identifier d'éventuels transferts[242] de données vers des pays « tiers ».
5. Préciser par écrit vos instructions et vous assurer que le contrat conclu avec votre sous-traitant prévoit des stipulations suffisantes encadrant ses obligations en matière de protection des données personnelles. Un modèle d'instructions écrites figure en annexe de la présente fiche.

[239] Le sous-traitant est défini à l'article 4 § 8 du RGPD comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

[240] Les fournisseurs qui agissent en qualité de responsable du traitement sont de fait soumis aux obligations prévues par la Règlementation applicable.

[241] Pour rappel, le simple accès à des données à caractère personnel est constitutif d'un traitement de données au sens de la Règlementation applicable.

[242] Le transfert international de données est défini par la CNIL comme *« toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'union européenne ».* Pour plus d'informations, consultez la Fiche 7 du Guide *« Transferts internationaux »*.

Gestion de la sous-traitance

Sommaire

1. Vérifier si votre prestataire/fournisseur traite de données à caractère personnel ou non

Ne sont concernés par la Règlementation applicable que les sous-traitants qui traitent des données à caractère personnel[243] :

Soit le prestataire ne traite aucune donnée à caractère personnel, alors le RGPD et la Loi informatique et liberté ne s'appliquent pas puisqu'il ne s'agira pas d'un sous-traitant au sens du RGPD.

Soit le prestataire met en œuvre un traitement de données à caractère personnel, auquel cas il convient de déterminer en quelle qualité il agit (responsable du traitement, responsable conjoint du traitement, ou sous-traitant).

2. Déterminer le statut de votre prestataire/fournisseur au sens du RGPD (sous-traitant ou responsable de traitement)

Le « sous-traitant » (au sens RGPD) est défini à l'article 4 § 8 du RGPD comme *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel* ***pour le compte*** *du responsable du traitement ».*

Dans le cadre de ses missions, le commissaire aux comptes peut avoir plusieurs sous-traitants au sens de la Règlementation applicable tels que des prestataires informatiques (éditeurs de logiciels d'audit, sous-traitant au sens du H3C (2010 06 24 Avis), hébergeurs, outils de *data mining*…) ou d'autres prestataires et fournisseurs (tels que les actuaires, organisateurs d'événements professionnels…).

Vous devez vous interroger sur la nature des prestations en question afin de vous permettre d'évaluer le statut du prestataire au regard du RGPD et des lignes directrices du CEPD.

> *À noter :* Tous vos fournisseurs n'agissent pas en qualité de sous-traitants au sens du RGPD[244]. Certains fournisseurs ne traitent des données à caractère personnel qu'à titre accessoire, c'est-à-dire exclusivement dans le cadre de l'exécution des prestations. Vos relations avec eux seront alors celles de responsable du traitement à responsable du trai-

[243] Les « données à caractère personnel », au sens de l'article 4 § 1 du RGPD sont définies comme *« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou un ou plusieurs éléments spécifiques propres à son identifié physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».*

[244] EDPB Guidelines 07/2020 on the concept of controller and processor in the GDPR – adopted on September 2nd 2020, § 80 : *« The EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a "processor" within the meaning of the GDPR. The role of processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. (…) In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor".*

tement (comme par exemple un fournisseur de documentation interactive, une plateforme de réservation de taxi)[245]. Dans ce cas de figure, la société de taxi est maître de sa plateforme et des données nécessaires pour fournir le service en question. La société de taxi n'est pas votre « sous-traitant » au sens du RGPD. (Pour plus d'informations sur les notions de responsable du traitement et de sous-traitant, vous pouvez vous référer aux lignes directrices du CEPD[246]).

Pour un rappel sur la qualification de responsable du traitement, consultez la Fiche n° 2 du guide *« Statut du commissaire aux comptes »*.

Il est recommandé de tenir une liste à jour de vos sous-traitants. Cette liste fait partie de votre documentation « accountability » (Cf. Fiche n° 1 du guide *« Gouvernance et Accountability »*).

3. Identifier les catégories de données personnelles auxquelles le sous-traitant a accès

Il convient également de déterminer le type de données que le sous-traitant est amené à traiter. Lorsqu'un sous-traitant traite des catégories particulières de données[247], des mesures renforcées de sécurité doivent être mises en place. Tel est le cas par exemple des données relatives aux condamnations pénales d'un dirigeant.

4. Connaître son sous-traitant

Avant de contracter avec un sous-traitant, il convient de se renseigner sur lui et de vérifier le sérieux de son activité au regard de la Règlementation applicable.

Une visite sommaire de son site internet peut permettre de déterminer si le sous-traitant dispose de mentions légales, d'une politique de confidentialité claire et complète, de bandeaux cookies, etc. Vous pouvez également demander une copie des certificats dont il dispose, des informations sur les mesures de sécurité qu'il met en place, des précisions sur les transferts de données qu'il opère, ses propres sous-traitants, etc.

Cela est d'autant plus nécessaire qu'en tant que responsable du traitement, vous êtes responsable de vos sous-traitants à l'égard des personnes concernées.

[245] En cas de discussion quant à la qualification juridique d'un fournisseur, conservez une trace des échanges (legal opinion, consultations juridiques, etc.).
[246] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
[247] Telles que les données sensibles (informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé, les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique).

5. Localiser les activités de sous-traitance

En tant que responsable du traitement, vous devez savoir où se trouvent les données personnelles que vous traitez et/ou sous-traitez, qui y accède et depuis quel pays. Localiser géographiquement vos sous-traitants permet d'identifier les éventuels transferts de données personnelles vers des pays tiers n'assurant pas un niveau de protection adéquat (Cf. Fiche n° 7 du guide *« Transferts internationaux »*).

Il convient de distinguer les pays bénéficiant d'une décision d'adéquation de ceux ne bénéficiant pas d'une telle décision :

- Si le sous-traitant est situé dans un pays tiers bénéficiant d'une décision d'adéquation (comme le Japon par exemple), le traitement peut avoir lieu sans garantie spécifique.
- Si le sous-traitant est situé dans un pays tiers ne bénéficiant pas d'une décision d'adéquation (comme Singapour par exemple), le traitement ne peut avoir lieu qu'**après** la mise en œuvre de l'une des **garanties appropriées** énumérées à l'article 46 du RGPD (clauses contractuelles types, BCR, Code de conduite…).

Il convient d'être vigilant à l'égard de vos sous-traitants situés aux États-Unis ainsi qu'aux hébergeurs soumis au *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*[248]. Pour plus d'informations, consultez la Fiche n° 7 du guide *« Transferts internationaux »*.

6. Contractualiser vos relations avec le sous-traitant

Le fait de confier des données à caractère personnel à un sous-traitant vous impose de contractualiser en ce sens[249]. Cela prendra la forme soit d'un contrat de sous-traitance à part entière, soit d'une clause et/ou une annexe à un contrat déjà existant[250].

> *À noter :* le contrat/la clause de sous-traitance fait partie de la documentation susceptible d'être demandée par la CNIL en cas de contrôle.
>
> (Cf. Fiche n° 1 du guide RGPD *« Gouvernance et Accountability »*, Fiche 9 *« Contrôles et sanctions de la CNIL »* et Fiche RGPD de la CNCC n° 5 *« Sécurisez vos relations avec vos prestataires »*).

[248] Le *CLOUD Act* est une législation américaine qui, sous certaines conditions, permet aux autorités américaines d'enjoindre à une entreprise soumise au droit US de communiquer des données personnelles qu'elle traite, y compris si ces données sont stockées sur des serveurs situés en dehors du territoire des États-Unis.
[249] Article 60 de la Loi informatique et libertés : *« Le traitement réalisé par un sous-traitant est régi par un contrat ou tout acte juridique qui lie le sous-traitant à l'égard du responsable du traitement, sous une forme écrite, y compris en format électronique, respectant les conditions prévues à l'article 28 du règlement ».*
[250] Article 28 § 3 du RGPD.

Ce contrat doit préciser les informations suivantes[251] :

– L'objet du traitement.

– La durée du traitement.

– La nature et la finalité du traitement.

– Le type de données à caractère personnel.

– Les catégories de personnes concernées.

– Les principales obligations du sous-traitant, telles que prévues à l'article 28 du RPGD.

Il est également recommandé d'indiquer dans le contrat de sous-traitance un point de contact privilégié chez chacune des parties concernant les questions relatives au traitement des données personnelles (en général, il s'agira de l'adresse mail du délégué à la protection des données).

Il existe plusieurs modèles de contrat de sous-traitance. La CNIL propose un modèle de clause/contrat de sous-traitance.

En toute hypothèse, les stipulations contractuelles doivent couvrir a minima les thématiques suivantes :

⇒ **Traitement pour votre compte et selon vos instructions[252]**

Le sous-traitant traite les données **pour le compte** du responsable du traitement et **sur instructions** de ce dernier. Ces instructions doivent préciser en particulier :

– **La finalité** du/des traitement(s),

Par exemple : la finalité du traitement mis en œuvre par un hébergeur a pour finalité le stockage des données personnelles.

– **La nature** du traitement (collecte, enregistrement, organisation, structuration, conservation, adaptation ou modification, extraction, consultation, utilisation, rapprochement ou interconnexion, effacement ou destruction).

– **Les catégories de données personnelles concernées.**

– **La durée** du/des traitement(s) et celle de conservation des données par le prestataire.

> *À noter :* votre contrat doit prévoir une durée de conservation des données par le sous-traitant et le sort des données à la fin du contrat (restitution et/ou destruction).

– **Les mesures de sécurité** mises en œuvre.

⇒ **Confidentialité[253]**

Le sous-traitant doit s'engager à respecter la confidentialité des données confiées notamment en mettant en place les mesures techniques et organisationnelles appropriées et/ou en soumettant les personnes habilitées à traiter lesdites données à une obligation légale appropriée de confidentialité.

[251] Article 28 § 3 du RGPD.
[252] Article 28 § 3 (a) du RGPD.
[253] Article 28 § 3 (b) du RGPD.

En tant que commissaire aux comptes, vous êtes soumis à des obligations déontologiques, et notamment au secret professionnel. À cet égard, vous devez répercuter le même niveau d'exigence à l'égard de vos sous-traitants.

⇒ **Sécurité des données[254]**

Le sous-traitant s'engage à prendre toutes les mesures de sécurité requises en vertu de l'article 32 du RGPD.

Celui-ci énumère une liste de mesures de sécurité à mettre en place pour assurer la sécurité des données, telles que la pseudonymisation, la réalisation de tests de sécurité, etc.

Pour plus d'informations sur la sécurité des données, vous pouvez consulter le Guide de la sécurité des données personnelles de la CNIL, le « Kit de la sécurité des données » de l'ANSSI, ainsi que la Fiche 8 du présent Guide *« Gestion de la sécurité des données »*.

À noter : En tant que responsable du traitement, vous êtes responsable de vos sous-traitants à l'égard des personnes concernées et de vos clients.

⇒ **Collaboration avec le responsable du traitement[255]**

Le sous-traitant doit aider et assister le responsable du traitement à *« garantir le respect des obligations prévues aux articles 32 à 36 du RGPD »*[256]. Cela implique notamment pour le sous-traitant de :

- Notifier toute violation de données au responsable du traitement[257] (Pour un rappel sur les règles en matière de notification des violations de données, voir la Fiche n° 6 du guide *« RGPD dans un contexte co-CAC »*).
- Aider le responsable du traitement dans le cadre des demandes d'exercice de droits dont les personnes concernées le saisissent[258]. Dans l'hypothèse où le sous-traitant recevrait directement une demande d'exercice de droits émanant d'une personne concernée, le sous-traitant doit la transférer au responsable du traitement. En toute hypothèse, le sous-traitant doit collaborer avec le responsable du traitement pour résoudre la demande d'exercice de droits à laquelle le responsable du traitement seul doit répondre.
- Aider le responsable du traitement à l'occasion d'un contrôle diligenté par l'autorité de contrôle ou dans la réalisation d'une analyse d'impact relative à la protection des données[259].

[254] Article 28 § 3 (c) du RGPD.
[255] Article 28 § 3 (f) du RGPD.
[256] Article 28.3 (g) du RGPD.
[257] Article 33.2 du RGPD *« le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance ».*
[258] Article 28.3 e) du RGPD *« le sous-traitant aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ».*
[259] Article 35 du RGPD.

⇒ **Conservation limitée**[260]

Le sous-traitant doit respecter la durée de conservation et les modalités prévues au contrat ainsi que celles prévues à la fin du contrat (destruction/restitution).

Le sort des données à la fin de la prestation doit donc être contractuellement prévu (qu'il s'agisse du terme du contrat ou d'une résiliation anticipée pour quelque raison que ce soit).

Il est recommandé de demander au sous-traitant de certifier par écrit la suppression des données à la fin du contrat.

⇒ ***Accountability***[261]

Le sous-traitant doit s'engager à mettre à votre disposition toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits.

En pratique, il s'agit pour le sous-traitant de tenir sa documentation *« accountability »* à disposition du responsable du traitement (telle que par exemple, les mesures de sécurité qu'il met en place, les opérations de traitement qu'il réalise, son registre des traitements, sa politique de confidentialité, ses contrats de sous-traitance ultérieurs, etc.).

Cela implique également le droit pour le responsable du traitement de **procéder ou faire procéder à un audit** de son sous-traitant.

⇒ **Ne pas recourir à un sous-traitant ultérieur sans l'autorisation préalable du responsable du traitement**[262]

Le sous-traitant doit s'engager à ne pas recruter d'autres sous-traitants sans votre autorisation écrite, préalable, spécifique (pour chaque sous-traitant ultérieur) ou générale (pour l'ensemble des futurs sous-traitants ultérieurs).

Lorsque la marge de négociation vous le permet il est recommandé de prévoir une liste des sous-traitants ultérieurs autorisés à annexer au contrat.

> *À noter :* si les sous-traitants ultérieurs sont situés dans un pays en dehors de l'Union Européenne, il conviendra de faire application des règles relatives aux transferts internationaux de données (Cf. Fiche n° 7 du guide *« Transferts internationaux »*).

Comment faire si je n'ai pas de marge de négociation face au sous-traitant ?

Il peut arriver de contracter avec des sous-traitants qui sont des acteurs majeurs du marché (notamment des hébergeurs, des éditeurs de logiciels…) qui ne laissent pas de place à la moindre modification de leurs contrats/conditions générales.

[260] Article 28 § 3 (g) du RGPD.
[261] Article 28 § 3 (h) du RGPD.
[262] Article 28 § 2 du RGPD.
[263] CNIL délibération n° 2014-298 du 7 août 2014 : la CNIL a prononcé un avertissement public à l'encontre de la société ORANGE en lui reprochant notamment de ne pas avoir réalisé d'audit de sécurité sur la version de l'application développée par son prestataire pour répondre à ses besoins. Cette décision a été confirmée par le Conseil d'État dans un arrêt du 30 décembre 2015.

En pareille situation, il convient de :

1. Vérifier que le sous-traitant est bien un acteur majeur du marché.
2. Vérifier que le contrat proposé par ce sous-traitant comporte des stipulations adéquates sur les thématiques susvisées.
3. Lire et conserver sa politique de confidentialité.
4. Lire et conserver ses informations et documents fournis en matière de sécurité et de transferts internationaux (certificats, politique de sécurité, clauses contractuelles types…).

Rappel : En tant que responsable du traitement, vous êtes responsable des défaillances de vos sous-traitants à l'égard des personnes concernées et de vos clients[263]. Vous devez vous assurer que votre sous-traitant respecte les mesures de sécurité prévues au contrat et dispose d'une assurance adaptée destinée à couvrir ses défaillances.

Annexe – Modèle d'instructions écrites du responsable du traitement au sous-traitant

	Nature du traitement	Finalité(s) du traitement	Types de données personnelles traitées	Catégories de personnes concernées	Mesures de sécurité à mettre en place	Durée de conservation et sort des données à l'issue du traitement	Lieu du traitement et éventuels transferts	Sous-traitant(s) ultérieur(s)[264]
Traitement n° 1 *(Nom du traitement)*	*Traitement automatisé/ non-automatisé*	*Ex. : Maintenance de logiciel*	*Ex. : Nom ; prénom ; adresse IP ; login…*	*Ex. : salariés, clients finaux, utilisateurs…*	*Ex. : pseudo-nymisation, anonymisa-tion…*	*Pendant toute la durée des relations contractuelles. Sort des données : restitution/destruction (avec attestation de destruction).*	*Ex. : France, Inde, États-Unis…*	
Traitement n° 2 *(Nom du traitement)*	*Traitement automatisé/ non-automatisé*	*Ex. : Gestion de la paie*	*Nom ; prénom ; n° de Sécurité sociale, adresse pos-tale…*	*Ex. : salariés, stagiaires…*	*Ex. : pseudo-nymisation, anonymisa-tion…*	*Pendant toute la durée légale de conservation incombant à l'employeur, prorogée des délais légaux de prescription.*		
Traitement n° 3 *(Nom du traitement)*	*Traitement automatisé/ non-automatisé*	*Gestion du fichier clients/ prospects*	*Nom ; prénom ; adresse IP ; login…*	*Ex. : prospects, clients…*	*Ex. : pseudony-misation, ano-nymisation…*	*Pendant une durée maximale de 3 ans à compter de la dernière sollicitation commerciale au prospect.*		

[264] Les sous-traitants dits ultérieurs sont les éventuels sous-traitants de votre prestataire.

N° d'Imprimeur : 83142

Impression Compédit Beauregard

Guides Professionnels

LES COMMISSAIRES AUX COMPTES
bâtisseurs d'une société de confiance

www.cncc.fr

200 - 216 rue Raymond Losserand
75680 Paris cedex 14
+33 (0)1 44 77 82 82

SERVICE ÉDITION
Ventes, informations sur les ouvrages

Tél. : 01 44 77 81 40
cnccservices.edition@cncc.fr

CNCC DÉPARTEMENT TECHNIQUE
question.juridique@cncc.fr