CODE DE CONDUITE DE L'ALLIANCE DU COMMERCE

Version du 27/01/2026

Code de conduite national approuvé par la CNIL le 12 février 2026 (délibération 2026-013)

CHAPITRE 1 – PRÉAMBULE

1. **Le secteur de l'habillement, des achats au centre des priorités des consommateurs**. Le secteur de l'équipement de la personne constituant l'un des premiers postes d'achat des consommateurs, ces derniers bénéficient quotidiennement des produits et des services qui y sont liés, désormais facilités grâce au développement de plusieurs canaux d'achat sur internet (e-commerce, *click & collect* et e-réservation), venus compléter le commerce traditionnel de la vente physique. Du fait de cette évolution, les données à caractère personnel sont de plus en plus collectées et exposées.

2. **La première organisation professionnelle française**. En qualité de représentant des acteurs du commerce, l'Alliance du Commerce est la première organisation professionnelle représentative du commerce de détail d'équipement de la personne en France (ci-après « **l'Alliance du Commerce** » ou le « **Porteur du Code** »). Elle est composée de trois fédérations, compte plus de sept cents enseignes et soixante-dix entreprises adhérentes (*pour une liste exhaustive de ses membres, voir https://www.alliancecommerce.org/nos-membres/*).

3. **La conformité au RGPD au cœur des préoccupations des adhérents**. Ses entreprises adhérentes étant quotidiennement confrontées aux exigences en matière de protection des données de leurs consommateurs, l'Alliance du Commerce a identifié auprès de ces dernières un besoin d'accompagnement et de soutien dans l'application des dispositions de la législation européenne relative à la protection des données.

4. **Le choix d'adopter un outil de conformité aisément compréhensible, qui ne dispense en rien de respecter le droit national et le RGPD**. Conformément à l'article 40 du Règlement (UE) n°2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après le « **RGPD** »), l'Alliance du Commerce a initié la rédaction de ce code de conduite (ci-après le « **Code** » ou « **Code de conduite** ») applicable au secteur de la vente au détail d'équipements de la personne. A cet effet, ce Code a vocation à constituer un outil de conformité pour les enseignes de l'Alliance du Commerce, dont la bonne application leur permet de démontrer leur conformité au RGPD, dans les limites strictes du périmètre matériel et territorial défini au sein du présent document. En conséquence, le Code ne saurait valoir dispense des enseignes de se conformer aux exigences posées par le RGPD non couvertes par le Code.

5. **Une adhésion volontaire, mais contraignante par son application, et destinée uniquement aux membres de l'Alliance du Commerce**. La demande d'adhésion au Code s'effectue sur une base de volontariat dans les formes prescrites au sein du présent document. Ce Code revêt, en revanche, un caractère contraignant pour toute enseigne qui y adhère librement en vertu de la procédure ci-après exposée[1]. Pour adhérer au présent Code, il est impératif d'être adhérent à l'Alliance du Commerce.

6. **La CNIL, autorité de contrôle désignée**. Conformément à l'article 55 du RGPD, la Commission Nationale de l'Informatique et des Libertés (« **CNIL** ») est l'autorité de contrôle compétente qui

[1] Lignes directrices adoptées par le CEPD le 4 juin 2019, à propos des codes de conduite, page 27&28.

(i) a approuvé le contenu du présent code, et (ii) a accordé l'agrément à l'organisme de suivi (le cas échéant), chargé de contrôler la bonne application de celui-ci (conformément à l'article 41 du RGPD). La CNIL a accompagné le porteur dans l'élaboration du Code en fournissant des recommandations sur ce dernier pendant toute la durée du processus de rédaction. **Le périmètre du code** porte uniquement sur les activités de traitement réalisées par un magasin ou une enseigne établie en France, agissant en qualité de responsable de traitement.

7. **Un Code élaboré grâce à la constitution d'un groupe de travail.** Le Code a été préparé dans le cadre d'une initiative portée par une quinzaine d'entreprises adhérentes à l'Alliance du Commerce, que cette dernière a rebaptisé le « Club DPO », lesquelles ont pu exprimer leurs attentes et leurs besoins en collaboration avec l'Alliance du Commerce tout au long du processus de rédaction du présent document. Le Club DPO a notamment fait valoir la nécessité de disposer d'un outil interne, qui soit un référentiel pratique, simple et opérationnel : en effet certaines entreprises ont particulièrement souligné la nécessité de disposer d'un recueil pratique, unique, détaillé et compréhensible, applicable à leur domaine d'activité, disposé à les mettre en mesure de fournir des éléments techniques et précis aux opérationnels, tandis que d'autres entreprises ont exprimé leur souhait d'obtenir un support de communication clair et opérationnel destiné à emporter l'adhésion grâce à la confiance qu'il pourrait générer parmi les entreprises adhérentes.

8. **Un outil encouragé selon la consultation des professionnels menée**. En parallèle, l'Alliance du Commerce a entrepris de mener une consultation auprès de ses entreprises adhérentes. 83% ont indiqué l'utilité certaine d'un code de conduite spécifique au secteur du commerce de détail d'habillement et de chaussure, la position de l'Alliance du Commerce en qualité de Porteur du Code ayant été amplement confortée (96%). Alors que certains ont évoqué leur aspiration à bénéficier, de la part de la CNIL, d'informations aussi pertinentes que celles des livres blancs mais portant plus spécifiquement sur le secteur de l'habillement et de chaussure, le besoin d'accéder à une analyse du RGPD qui soit adaptée au secteur d'activité s'est fait ressentir dans de nombreux commentaires. Ces attentes s'illustrent dans le Code, qui couvre les relations B2C cœur de métier. En revanche, malgré les manifestations des intéressées d'obtenir un accompagnement dans leurs relations B2B, avec leurs fournisseurs de services, le choix a été fait d'exclure ces derniers, en concertation avec la CNIL. Ainsi, 88% des entreprises adhérentes de l'Alliance parties prenantes se sont déclarées intéressées pour adhérer au Code, se sont engagées à l'appliquer, et souhaiteraient même communiquer auprès de leurs interlocuteurs sur leur adhésion, gageant ainsi de leur conformité au RGPD.

9. Une synthèse des consultations des acteurs est présentée en **Annexe F**.

10. **Sommaire du Code**.

Le présent Code adopte le plan suivant :

CHAPITRE 1 – PRÉAMBULE 2
1.1 Présentation du Porteur du Code et du secteur concerné 5
1.2 Représentativité du Porteur du Code 6
1.3 Objectifs poursuivis 8
1.4 Périmètre 9
CHAPITRE 2 – LES PRINCIPES FONDAMENTAUX DE LICEITE 16
2.1. Des finalités déterminées et légitimes pour le secteur 16
2.2. Des traitements proportionnés pour le secteur 29
CHAPITRE 3 – LES OBLIGATIONS 43
3.1. Information des personnes concernées 43
3.2. Procédures d'exercice des droits des personnes concernées 52
3.3. Encadrement des contrats entre acteurs de traitement 60
3.4. Encadrement des Transferts de Données Personnelles en dehors de l'Union Européenne 71
3.5. Obligation de sécurité 75
3.6. Registre des traitements 88
3.7. Délégué à la protection des données personnelles (DPO) 88
CHAPITRE 4 – GOUVERNANCE DU CODE 95
4.0. Organes internes 95
4.1. Organisme(s) de contrôles externes 97
4.2. Contrôle du respect du code 101
4.3. Information de l'autorité de contrôle compétente 105
4.4. Délais 106
CHAPITRE 5 – DECLARATION DE CONFORMITE 107
5.1. Processus d'adhésion au Code 107
5.2. Documentation 108
5.3. Marque de conformité 108
CHAPITRE 6 – RETRAIT D'ADHESION 110
CHAPITRE 7 – COMMUNICATION ET PUBLICATION DU CODE 111
CHAPITRE 8 – MODIFICATION DU CODE 112

1.1 Présentation du Porteur du Code et du secteur concerné

1.1.1. Le Porteur du Code, l'Alliance du Commerce

11. **Un groupement constitué d'associations**. L'Alliance du Commerce est un groupement d'intérêt économique (GIE), constituée par trois associations régies par la loi du 1er juillet 1901, la Fédération des Enseignes de l'Habillement (FEH), la Fédération des Enseignes de la Chaussure (FEC) et l'Union du Grand Commerce de Centre-Ville (UCV). Il s'agit de la première organisation professionnelle dans l'équipement de la personne, dirigée par Monsieur Yohann PETIOT, Directeur général.

12. **Des associations fédérant le marché de l'habillement et de la chaussure**. En 2021, l'Alliance du Commerce réunissait plus de 750 enseignes présentes sur 27 000 points de vente, comprenant trois branches professionnelles composées des grands magasins et des magasins populaires, ainsi que des enseignes de l'habillement et de la chaussure. A cette même date, l'ensemble de ces enseignes employait plus de 170 000 personnes et générait un chiffre d'affaires de 41 milliards d'euros environ (voir https://www.alliancecommerce.org/alliance-du-commerce/).

13. **Un groupement s'inscrivant dans les mutations imposées par la transformation digitale, le développement durable et l'apparition de nouveaux modes de consommation**. L'Alliance du Commerce agit pour un commerce innovant et responsable, déployé par la mise en œuvre de diverses missions qui lui incombent et ci-après listées :

    - La représentation des intérêts des adhérents : l'Alliance du Commerce agit auprès du gouvernement, des pouvoirs publics et d'autres organisations professionnelles pour assurer un environnement économique et social favorable au développement des acteurs du commerce ;

    - La promotion du commerce : l'Alliance du Commerce est le porte-parole de la profession auprès des médias et du grand public ;

    - L'animation du dialogue social : l'Alliance du Commerce, par les fédérations qui la composent, intervient dans les négociations sectorielles aux côtés des syndicats salariés et des pouvoirs publics afin de faire évoluer les métiers de la vente ;

    - L'information des adhérents : l'Alliance du Commerce fournit aux adhérents une expertise législative et juridique des évolutions réglementaires, économiques et sociales du secteur ;

    - La facilitation des échanges : l'Alliance du Commerce apporte aux adhérents des solutions concrètes face aux défis et problématiques rencontrées par les acteurs du commerce.

1.1.2. Le secteur concerné, la vente et la distribution au détail de produits d'équipements de la personne

14. **Un secteur à la convergence de trois fédérations**. Le secteur français de la vente et la distribution au détail de produits d'équipements de la personne se concentre autour de trois fédérations se répartissant le commerce de l'habillement, d'articles textiles et d'articles chaussants :

- L'Union du Grand Commerce de Centre-Ville (UCV) regroupe tous les grands magasins et les magasins populaires, dont les enseignes proposent une offre variée de produits de la mode et du luxe, mais également de produits alimentaires, de culture, loisirs. En 2025, elle compte cinq grandes enseignes (Galeries Lafayette, Le Bon Marché, Monoprix, le Printemps, Samaritaine) attirant une clientèle urbaine et touristique.

- La Fédération des Enseignes de l'Habillement (FEH) regroupe les grandes chaînes françaises de l'habillement. Occupant une part de marché de près de 50%, les six cents enseignes adhérentes sont des leaders de la vente d'habillement, l'un des premiers postes de consommation des Français.

- La Fédération des Enseignes de la Chaussures (FEC) regroupe, en 2025, plus d'une centaine d'enseignes françaises spécialisées dans l'équipement chaussant de la personne.

1.2 Représentativité du Porteur du Code

15. **L'Alliance du Commerce, un organe représentatif certifié par arrêté**. Conformément à la réforme de la représentativité patronale menée par la Loi du 5 mars 2014, l'Alliance du Commerce se voit reconnaître sa représentativité patronale, par arrêté pour une durée de 4 années (2025-2028) et pour chacune de ses 3 fédérations :
    - Pour la Fédération des Enseignes de l'Habillement : arrêté du 17 juillet 2025 concernant la convention collective nationale des maisons à succursales de vente au détail d'habillement,
    - Pour l'Union du Grand Commerce de Centre-Ville : arrêté du 1er octobre 2025 concernant la convention collective nationale des grands magasins et des magasins populaires,
    - Pour la Fédération des Enseignes de la Chaussure : arrêté du 24 juin 2025 concernant la convention collective nationale du commerce succursaliste de la chaussure.

16. Pour une information complète, pour l'année 2024, le rapport de branches de la FEH permet de comptabiliser : 190 804 salariés de la branche de l'Habillement, composant plus de 1 124 entreprises, réparties sur 14 201 points de vente, dont 40% situés en centre-ville et 47% dans les centres commerciaux ; et 32 364 salariés de la branche de l'Union du Grand Commerce de Centre-Ville, composant quatre principales enseignes (Le Bon Marché, les Galeries Lafayette, le Printemps pour les Grands Magasins ; Monoprix pour les Magasins populaires ; la Samaritaine),

réparties sur environ 400 points de vente et générant près de 8 milliards d'euros de chiffres d'affaires annuel[2].

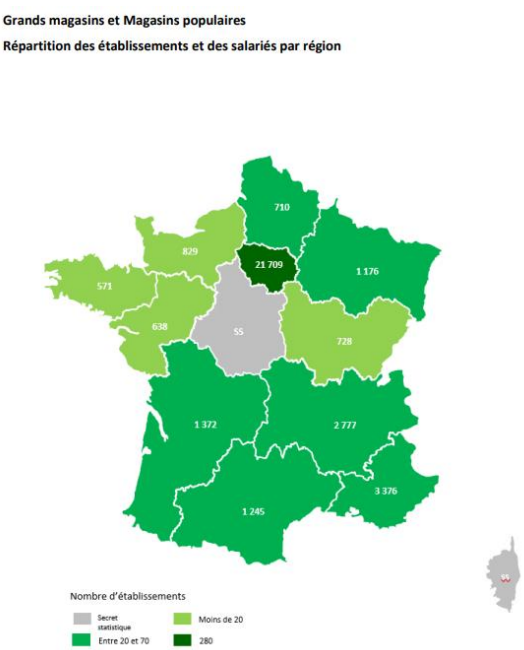
17. **Un secteur habillement déployé à l'international**. En plus de son déploiement sur l'ensemble du territoire national, une des principales caractéristiques de la branche est sa forte présence à l'international : en 2019, les exportations françaises d'habillement dans leur ensemble ont affiché une croissance de 5% par rapport à 2018. Les exportations vers l'Asie (notamment la Chine et Hong-Kong) ont crû de 14% et totalisent à elles seules 13,7% des exportations françaises d'habillement.

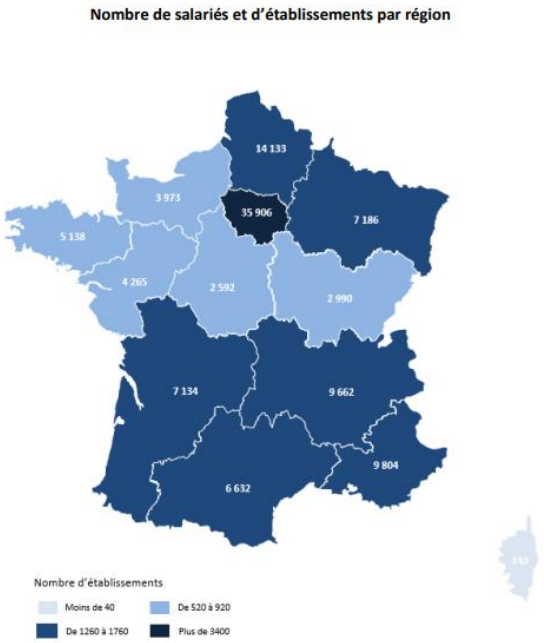
18. **La transformation digitale du commerce de l'habillement**. Le commerce de l'habillement est également marqué par la digitalisation de son économie. Les enseignes physiques sont ainsi passées à la vitesse supérieure sur internet et se sont investies dans l'omnicanal ces dernières années. Elles créent des boutiques en ligne et adaptent leur stratégie e-commerce à l'intensification de la concurrence des *pure player* et des entreprises de vente à distance. En effet, les ventes en ligne d'habillement et textile ont connu une croissance soutenue (+25% en 2024 vs 2019). En France, les produits les plus vendus en ligne sont l'habillement enfant, la lingerie, l'habillement femme et l'habillement homme.

19. **L'apparition de nouveaux modes de consommation**. Les professionnels du secteur sont confrontés à des enjeux d'évolution des modes de consommation liée notamment à l'utilisation croissante de nouveaux moyens technologiques (e-commerce, tablettes, …), à la prise en compte de problématiques sociétales et environnementales ou encore au tourisme. Les entreprises doivent d'ores et déjà s'adapter aux futurs modes de consommation, de commercialisation et de gestion des stocks et de la logistique sans que les contours de ces changements permanents et rapides ne soient aujourd'hui connus.

20. **Une disparité d'établissements**. Les deux cartes ci-dessous retracent le nombre d'établissements présents par région française, et le nombre de salariés associés. A titre d'exemple, cette représentation permet de mettre en exergue une concentration d'établissements toute branche confondue dans la région Ile-de-France avec des disparités territoriales marquées par une présence bien plus faible dans les régions du milieu de la France.

[2] Rapport de branche, Edition 2025 – CPPNI FEH – présenté le 1er décembre 2025





1.3 Objectifs poursuivis

21. **La création d'un outil de confiance**. Ce Code vise ainsi à créer un environnement de confiance et à maintenir le degré le plus élevé de protection des données pour le périmètre précisément déterminé au titre suivant. Instrument volontaire mais contraignant une fois son adhésion entérinée, cet outil de bonnes pratiques, qui unifie les interprétations en matière de données personnelles, a vocation à légitimer les demandes formulées par les représentants des enseignes en charge des problématiques de données personnelles auprès des divers services internes quotidiennement confrontés au traitement de ces données (marketing, commerciaux, logistiques, après-vente, juridique, comptabilité…), par une méthodologie harmonisée portée par l'Alliance du commerce.

22. **Un objectif de conformité partagée**. Ce Code est destiné à constituer un véritable levier interne de conformité au RGPD, en transcrivant cette réglementation de manière pratico-sectorielle, l'idée étant de parvenir à un consensus des enseignes autour d'une terminologie commune et surtout d'un niveau de conformité commun.

23. **Un Code non destiné à constituer un instrument de Transfert**. Le Code ne constitue pas un dispositif autorisant le Transfert de données à caractère personnel en dehors de l'Espace économique européen (EEE). Lorsque des données à caractère personnel sont transférées vers des pays non-membres de l'EEE, il convient d'utiliser un mécanisme de Transfert reconnu par le Chapitre V du RGPD.

1.4 Périmètre

1.4.1. Définitions

Le Code définit et précise les notions qu'il aborde (les termes identifiés par un astérisque correspondent à des notions définies par le RGPD) qui sont notamment complétées par les définitions prévues au sein de la boîte à outils, **Annexes A3** « Référentiel des catégories de personnes concernées » et **A6** « Référentiel des opérations de traitement » :

- ***Abonné*** : Personne physique ayant souscrit un abonnement pour un service tel que la réception d'une lettre d'information (newsletter) ou des campagnes marketing ;

- ***Annuaire d'Accès Informatique* (ou « AAI », aussi appelé « Active Directory », en référence au nom donné à cet outil par l'éditeur Microsoft)** : outil répertoriant les personnes ou catégories de personnes habilitées à accéder aux ressources informatiques de l'Enseigne ;

- ***Client (classique) :*** Personne physique ou morale bénéficiant de biens, de services ou d'un statut fourni ou conféré par le Responsable de traitement, avec ou sans contrepartie, ou bien s'engageant à les payer, et dont les données à caractère personnel sont conservées licitement (tel que défini en Annexe A3) ;

- ***Client Fidèle :*** Client classique s'étant juridiquement engagé pour bénéficier d'avantages commerciaux (programme de fidélité, par exemple). On parle également d'adhérents ;

- ***Client Parrain :*** Client classique participant à une opération commerciale lui procurant des avantages, par laquelle elle fait bénéficier un ou plusieurs tiers parrainés, aussi appelés filleuls, d'offres ou avantages divers ;

- ***Collecte :*** La collecte est le recueil de données à caractère personnel, pouvant s'effectuer notamment à l'aide de questionnaires, de formulaires, ou encore de dispositifs techniques tels que des traceurs/cookies ou des balises wifi/Bluetooth. Elle peut être qualifiée de directe, auquel cas elle s'effectue directement auprès de la personne concernée qui en est informée par le Responsable de traitement ; ou d'indirecte, ce qui correspond au cas où les données n'ont pas été recueillies directement auprès de la personne concernée et lors de laquelle le Responsable de traitement doit en informer la personne concernée ;

- ***Commerce de détail*[3] *:*** l'activité consistant à vendre des marchandises dans l'état où elles sont achetées (ou après transformations mineures) généralement à une clientèle de particuliers, quelles que soient les quantités vendues. Outre la vente, l'activité de commerce de détail peut recouvrir la livraison, l'installation et la réparation chez le client (meubles/électroménager). La commercialisation d'un bien comprend

[3] Selon la définition donnée par l'Institut national de la statistique et des études économiques (Insee)

généralement successivement une activité de commerce de gros suivie d'une activité de commerce de détail. La vente au détail, telle qu'elle est entendue au sens du présent Code, comprend la vente de seconde main ;

- ***Commerce électronique*[4] *:*** transaction commerciale utilisant internet ou autres réseaux informatiques comme l'échange de données informatisé et impliquant un changement de propriété du bien ou du service commandé. Les biens font l'objet d'une commande déposée via réseaux, tandis que le paiement et la livraison du bien peut s'effectuer par tout autre méthode traditionnelle ;

- ***Conservation :*** La conservation des données à caractère personnel correspond au stockage des données sous une forme permettant d'en faire un traitement, et ce dans une base active, ou bien en archivage intermédiaire, ou enfin en archivage définitif ;

- ***Cookies :*** petits fichiers qui sont envoyés vers le navigateur et enregistrés sur le disque dur du smartphone, de la tablette tactile, etc., lors de la connexion de l'Utilisateur au Site internet. Les cookies recouvrent les catégories suivantes : les cookies et des variables HTTP, qui peuvent notamment transiter par des pixels invisibles ou des "web beacon" ; les cookies « flash » ; les accès aux informations du terminal depuis des API (LocalStorage, IndexedDB, identifiants publicitaires tels que l'IDFA ou l'Android ID, l'accès au GPS, etc.), tout autre identifiant généré par un logiciel ou un système d'exploitation (numéro de série, adresse MAC, identifiant unique de terminal (IDFV), ou tout ensemble de données qui servent à calculer une empreinte unique du terminal (par exemple via une méthode de « fingerprinting »). Pour plus de simplicité, nous parlerons de façon générique de « Cookies » ;

- ***Destinataire :*** « *toute personne habilitée à recevoir communication* » des données, et qui est *« autre que : la personne concernée, le responsable de traitement, le Sous-traitant, et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données »*, et à l'exception des *« autorités légalement habilitées »* qui – lorsqu'elles agissent *« dans le cadre d'une mission particulière, ou de l'exercice d'un droit de communication »* - ne *« constituent pas des destinataires »* [5]. En d'autres termes, une personne peut être considérée comme destinataire du traitement, dès lors qu'elle est habilitée à accéder aux données. Cette notion recouvre donc deux cas de figure :

  - Soit le Destinataire participe à la chaîne de traitement initial : il ne sera donc pas un « tiers » et sera, par exemple, un service interne au responsable de traitement, ou son

[4] Selon la définition donnée par l'Institut national de la statistique et des études économiques (Insee)
[5] Article 4 § 9 RGPD : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des Destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement* ».

Sous-traitant. Il sera Destinataire du traitement des données, car il s'inscrit dans le traitement initial ;
- Soit le Destinataire reçoit communication des données en qualité de « tiers », afin de procéder ensuite à un nouveau traitement dont il sera seul ou co-responsable.

- ***Destruction (effacement)*** : La destruction ou l'effacement correspond au processus aboutissant à la disparition définitive des données à caractère personnel ;

- ***Display*** : affichage de contenus, le plus généralement utilisé à des fins publicitaires et apparaissant dans des espaces d'une page web vendus à cet effet à des annonceurs ;

- ***Enregistrement*** : L'enregistrement équivaut à la consignation des données collectées sur un registre public ou privé en vue de leur sauvegarde et leur préservation par le Responsable de traitement ;

- ***Enseignes :*** les entreprises exploitant une enseigne de commerce dans le secteur visé par le Code de conduite et qui décident de se soumettre au processus d'adoption du Code pour y adhérer ;

- ***Extraction :*** L'extraction correspond au retrait ou à la copie du contenu des données à caractère personnel à partir d'un support particulier ;

- ***Interconnexion :*** Mise en relation automatisée d'informations (c'est-à-dire rapprochement automatique) provenant de fichiers ou de traitements qui étaient au préalable distincts*. Il y a interconnexion de fichiers lorsque trois critères cumulatifs sont réunis :

    (i) L'objet de l'interconnexion doit être la mise en relation de fichiers ou de traitements de données à caractère personnel ;

    (ii) La mise en relation concerne au moins deux fichiers ou deux traitements distincts ;

    (iii) La mise en œuvre de moyens automatisés ayant pour objet de mettre en relation et/ou alimenter ces fichiers ou ces traitements par les informations obtenues issues respectivement de ces derniers.

- ***Limitation :*** La limitation concerne la restriction du traitement lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée, lorsque le traitement est illicite, lorsque le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement, ou encore si la personne concernée s'y est opposée ;

- ***Organisme de contrôle*** : Entité agréée par la CNIL pour procéder au contrôle de la conformité des enseignes qu'elle a en charge aux exigences du Code, dans les termes prévus au Chapitre 4 dudit Code ;

- ***Prospect :*** Personne physique identifiée comme pouvant être intéressée par des produits ou services fournis par le Responsable de traitement, et n'ayant pas encore acquis la qualité de Client, ou n'étant plus qualifié de Client (tel que défini en Annexe A3) ;

- ***Push :*** Diffusion d'une information auprès d'un destinataire qui la reçoit ; à titre d'exemple, l'envoi de messages de prospection commerciale par courriel, ou encore SMS, ou enfin par notification, constitue un traitement ayant pour finalité la publicité ciblée par push ;

- ***Rapprochement :*** Mise en relation entre deux bases de données mais qui ne suppose pas la mise en œuvre de moyens automatisés et peut être réalisé au sein d'un même fichier ou d'un même traitement ;

- ***Responsable de traitement :*** l'Enseigne traitant les données à caractère personnel de ses Clients et Prospects dans le respect du Code de conduite ;

- ***Sous-traitant* :*** 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 ;

- ***Tiers parrainé-Filleul*** : Personne physique concernée par une collecte indirecte de la part du responsable de traitement qui la fait bénéficier d'offres et avantages divers ;

- ***Transfert*** : Un transfert de données à caractère personnel hors de l'Union européenne est une opération de traitement consistant pour un exportateur responsable de traitement ou un sous-traitant (exportateur) soumis au RGPD pour le traitement en cause, à communiquer par transmission ou à rendre accessible par un autre moyen des données à caractère personnel à une organisation internationale ou un importateur responsable de traitement, responsable conjoint ou sous-traitant se trouvant dans un pays tiers, qu'il soit soumis ou non au RGPD pour le traitement en cause. ;

- ***Vendeur :*** Personne physique ou morale qui vend par l'intermédiaire du Responsable de Traitement (tel que défini en Annexe A3) ;

- ***Visiteur*** : Personne physique qui navigue sur le site internet du Responsable de traitement sans disposer d'un compte personnel ;

- ***Utilisateur*** : Visiteur disposant d'un compte personnel sur le site internet du Responsable de traitement.

1.4.2. Champ d'application géographique : le territoire français, centre de décision des Enseignes

24. Un code transnational désigne un code portant sur des activités de traitement dans plus d'un État membre, à l'inverse d'un code national[6].

25. **Un Code adressé aux établissements français**. S'agissant des Enseignes constituées de groupes d'entreprises comprenant des filiales et/ou un siège social à l'étranger, le Code ne s'adresse donc qu'aux établissements (entité siège / entité filiale) situés en France.

26. **Le critère du centre de décision**. Peuvent adhérer à un code de conduite français les acteurs de traitement dont les centres de décisions sont situés en France. L'Alliance du Commerce a déterminé le périmètre géographique français du présent Code, auquel ne pourront adhérer que les Enseignes procédant à des activités de traitements de données uniquement sur le territoire français. Pour autant, le présent code s'applique aux traitements dits transfrontaliers au sens de l'article 4, § 23 du RGPD[7].

1.4.3. Champ d'application matériel

27. **Un périmètre déterminé par le porteur**. Le périmètre matériel du Code est déterminé par le Porteur du code, l'Alliance du Commerce, à la lumière des intérêts et des besoins des professionnels du secteur, à savoir les Enseignes.

28. **Un Code strictement applicable aux Enseignes agissant en qualité de Responsable de traitement**. Le RGPD impose des obligations légales aux responsables du traitement et aux Sous-traitants, celles pesant sur les premiers étant plus vastes que celles pesant sur les seconds, lesquels peuvent jouer un rôle de soutien dans l'exécution des obligations des responsables du traitement. Dans le cadre de l'application du Code, les Enseignes sont qualifiées de Responsable de traitement pour les activités de vente directe ou de réparation auprès du Client final. Est donc exclue du champ d'application du Code, la situation dans laquelle les Enseignes sont qualifiées de Sous-traitant pour les activités pour lesquelles elles agissent en qualité de fournisseurs de service logistique auprès des Vendeurs, dès lors qu'elles interviennent dans la

[6] Ainsi, un code transnational peut porter sur des activités de traitement menées par un grand nombre de responsables du traitement ou de sous-traitants dans plusieurs États membres.

[7] Pour rappel, un traitement transfrontalier se définit comme :

(i) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres,

(ii) ou un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ;

Dans le cadre du présent Code, les Enseignes peuvent se trouver dans la deuxième situation (ii).

chaîne logistique de gestion des stocks, d'envoi des pièces commandées et du service client (l'entité marketplace a la qualité de Vendeur et l'Enseigne a la qualité de fournisseur du Vendeur). En conséquence, l'Enseigne récupère les données personnelles du Client final afin de lui livrer sa commande[8].

29. **Un Code uniquement applicable aux traitements « de base » liées à la vente**. Après échange avec les parties prenantes évoquées ci-avant, l'Alliance du Commerce souhaite donner la priorité aux traitements liés aux « activités de base », à savoir les traitements concernés par la vente et la distribution des produits d'équipements de la personne. Sont écartés du périmètre du Code de conduite :
    - Les traitements liés aux « activités supports », à savoir les traitements concernés par les départements internes RH,
    - Ainsi que les traitements liés à l'approvisionnement (gestion des fournisseurs), pour lesquels l'Alliance du Commerce considère que des référentiels sont aisément accessibles afin d'aider les professionnels, tous secteurs confondus, à adopter les bonnes pratiques.

30. **Boîte à outils : un instrument facultatif**. Additionnellement aux exigences posées par le Code, l'Alliance du Commerce met à la disposition des Enseignes une boîte à outils communiquée par voie électronique à ces dernières après adhésion, composé d'annexes d'application non contraignante, élaborées dans un objectif d'apporter aide, uniformisation de langage et illustrations de bonnes pratiques aux Enseignes. En conséquence :

    - Les Enseignes restent libres de les adopter en totalité, partiellement ou d'en adopter d'autres dans l'hypothèse où elles disposeraient déjà d'outils de conformité aboutis et appliqués ;
    - L'organisme chargé de la bonne application du Code, visé au Chapitre 4 – Gouvernance, ne saurait être lié par ces annexes dans le contrôle qu'il mène auprès des Enseignes. Il peut toutefois s'en référer s'il le souhaite.

    En toute hypothèse, les Enseignes, qui décideraient d'adopter d'autres mesures ou d'autres terminologies que celles proposées au sein de cette boîte à outils, s'engagent à prendre des mesures d'application équivalentes ou d'en appliquer le Code en cohérence avec leurs référentiels internes afin de lui permettre de démontrer sa conformité aux exigences du Code. Ces annexes sont composées des six référentiels pratiques ci-après listés et d'un modèle de registre de traitements à personnaliser :

    - Les sous-catégories de données à caractère personnel concernées par les traitements mis en œuvre par les adhérents au Code de conduite sont exhaustivement réparties selon la classification suivante :

        - Identités personnelle et professionnelle, justificatif d'identité, image ;
        - Situation familiale, habitudes de vie, préférences personnelles ;
        - Situation professionnelle, qualification ;

[8] Exemples de Veepee, the Bradery,etc.

- Revenus et charges, moyens de paiement, crédit ;
- Identifiants uniques, détails de l'achat client/transaction fournisseurs, navigation web, réseaux sociaux ;
- Détails des communications ;
- Géolocalisation ;
- Données relatives au service client ;
- Données sensibles concernant la santé ;

- Les catégories de personnes concernées, précisément définies, sont les Abonnés, les Clients (classiques, Fidèles, et Parrains), les Fournisseurs, les Prospects, les Tiers Parrainés/Filleuls, les Vendeurs, les Visiteurs, et les Utilisateurs (ci-après les « **personnes concernées** »).

- Les catégories de Destinataires sont exhaustivement listées selon qu'ils soient internes ou externes à l'Enseigne.

- Les finalités dans le secteur, organisées par processus / cycle sont la prospection, le commerce / vente, la fidélisation, la connaissance Client / la connaissance Prospect, la surveillance / sécurité.

- Les opérations de traitement, précisément définies, dont les spécifications constituent le cycle de vie de la donnée.

- Les canaux de Collecte présentés selon la qualification juridique de collecte directe ou indirecte que leur attribue le RGPD.

31. **Responsabilité du Porteur du Code**. L'Alliance du Commerce ne saurait voir sa responsabilité engagée en cas de non-respect du Code par une Enseigne pour quelque motif. L'Enseigne ne dispose d'aucun droit ou recours direct en vertu du Code de conduite ou en relation avec le Code de conduite à l'encontre du Porteur du Code.

32. **Communication**. La communication effectuée grâce à la Marque, qui exprime l'engagement de l'Enseigne de respecter les exigences du présent Code, ne saurait signifier une conformité au RGPD.

CHAPITRE 2 – LES PRINCIPES FONDAMENTAUX DE LICEITE

2.1. Des finalités déterminées et légitimes pour le secteur
2.1.1. Les bases légales admissibles
2.1.2. Le cas des traitements ultérieurs
2.1.3. Le cas des traitements soumis à analyse d'impact relative à la protection des données

2.2. Des traitements proportionnés pour le secteur
2.2.1. La minimisation des données
2.2.2. La minimisation des Destinataires
2.2.3. La limitation de Conservation dans le temps

33. **Rappel pédagogique**. En application de l'article 4 du RGPD, le responsable de traitement est celui qui prend l'initiative et pilote la finalité, ainsi que les moyens (techniques, humains, ou matériels tels que les données collectées, les durées de Conservation, les logiciels etc.)[9] liés à la mise en œuvre du traitement, tandis que le Sous-traitant est celui qui agit « *pour le compte du responsable de traitement* » et doit donc rigoureusement se conformer aux instructions de ce dernier.

34. L'ensemble des traitements identifiables tout au long du cycle de vie de la donnée, et mis en œuvre par les Enseignes au cours du parcours de la personne concernée, de son statut de Prospect à son statut de Client, sont réalisés par ces dernières en qualité de Responsable de traitement.

35. En effet, ce sont les Enseignes qui disposent du rôle décisionnel associé et déterminent de la manière dont sont traitées les données collectées pour chaque traitement.

36. Comme il est indiqué dans la partie « Champ d'application matériel », l'Enseigne peut également agir en qualité de Sous-traitant dans le cadre des activités de service logistique qu'elles réalisent auprès des Vendeurs. Le Code ne s'applique toutefois pas dans cette situation.

2.1. Des finalités déterminées et légitimes pour le secteur

2.1.1. Les bases légales admissibles

37. **RAPPEL DE LA RÈGLE POSÉE PAR LE RGPD.** Le Responsable du traitement doit s'assurer que les données à caractère personnel sont « traitées de manière licite » conformément à l'article

[9] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées le 7 juillet 2021. On entend par « moyens essentiels » ceux qui sont étroitement liés à la finalité et à la portée du traitement, tels que le type de données à caractère personnel qui sont traitées (« *quelles données sont traitées?* »), la durée du traitement (« *pendant combien de temps sont-elles traitées ?* »), les catégories de Destinataires (« *qui aura accès aux données ?* ») et les catégories de personnes concernées (« *à qui appartiennent les données à caractère personnel traitées ?* »).

5(1)(a) du RGPD. Aux termes de l'article 6 du RGPD, la licéité de chaque traitement est conditionnée au choix de sa base légale. Autrement dit, pour être licite, tout traitement doit :

- soit (i) être **nécessaire** :
  - au respect d'une **obligation légale**, incombant au Responsable de traitement ;
  - à l'**exécution d'un contrat** auquel la personne concernée est partie, ou de mesures précontractuelles prises à la demande de celle-ci ;
  - à la réalisation de l'**intérêt légitime** poursuivi par le Responsable de traitement ou d'un tiers, sous réserve de préserver les droits et les libertés fondamentaux de la personne concernée, selon une mise en balance (nature des données, caractère inattendu du traitement au regard des attentes raisonnables de la personne concernée, éventuelles conséquences négatives du traitement pour la personne, éventuelles garanties complémentaires[10]) ;
- soit (ii) avoir reçu le **consentement préalable** de la personne concernée, lequel doit avoir été recueilli de manière univoque, libre, spécifique et éclairé.

38. **Les indicateurs du choix de la base légale admissible**. Afin de déterminer la base légale admissible, l'Enseigne peut suivre le cheminement suivant :

- Le traitement mis en œuvre est-il rendu obligatoire par un texte (légal ou règlementaire) impératif, suffisamment clair et précis dans le cadre de l'activité métier[11] ? L'obligation légale doit alors être retenue pour ces traitements.
- Existe-t-il une relation contractuelle entre l'Enseigne et la Personne Concernée (ou une relation précontractuelle initiée par la Personne Concernée) et le traitement est-il objectivement nécessaire à l'exécution de contrat au regard de son objet[12] ? Dans ce cas, la base légale du contrat doit être retenue pour les traitements qui en découlent.
- Le traitement, qui n'est ni imposé par une disposition légale, ni mis en œuvre dans le cadre d'une relation contractuelle, est-il nécessaire pour répondre à un intérêt légitime de l'Enseigne ? Pour y répondre l'Enseigne doit procéder au test de mise en balance des intérêts, en répondant aux questions suivantes :
- Les intérêts sont-ils ou non légitimes (« *purpose test* ») ?
- Le traitement est-il nécessaire à la réalisation des intérêts poursuivis (« *necessity test* ») ?

[10] V. notamment Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (p. 34 et s.).

[11] A titre d'exemple, relèvent de ce fondement, les prestataires techniques tenus de conserver les données relatives à la création de contenus, en application du décret n°2011-2019 du 25 février 2011 (CE, 20 nov. 2013, n°347349) ; mais tel n'est pas le cas d'un fournisseur d'accès à internet qui a décidé de mettre en place un dispositif de blocage anti-spams, en l'absence de dispositions légales précises à ce sujet (T. Com. Paris, ord. réf. 20 janvier 2016).

[12] Il faut toutefois prêter attention au fait qu'un traitement de données, pour se fonder sur la base légale qu'est l'exécution du contrat, doit être strictement nécessaire à l'exécution du contrat : la présence d'un contrat ne suffit donc pas, encore faut-il que le traitement de données soit indispensable à l'exécution de celui-ci (CEPD, Lignes directrices du 2/2019 du 8 octobre 2019). A titre d'exemple, un commerçant ne pourra pas s'appuyer sur ce fondement pour établir un profil des habitudes ou préférences de consommation de ceux-ci, car un tel traitement n'est nullement rendu nécessaire pour l'exécution, *stricto sensu*, du contrat.

- Les droits fondamentaux ou les intérêts des personnes concernées sont-ils suffisamment protégés (« *balancing test* »), en tenant compte de leurs attentes raisonnables ?
- Quelles garanties supplémentaires sont mises en œuvre ?

Si les réponses à ces questions sont positives, le traitement répond dans ce cas à l'intérêt légitime de l'Enseigne, sous réserve du respect de certaines conditions.
Si aucune de ces étapes ne permet à l'Enseigne de retenir l'une des bases légales précitées, alors elle doit recueillir le consentement de la Personne Concernée.

A noter que, dans certains cas, des textes spécifiques prévoient l'obligation de recueillir le consentement des personnes pour certaines finalités. Il s'agit, par exemple, des dispositions applicables pour la prospection par voie électronique sous certaines conditions (article 34-5 du code des postes et des communications électroniques) ou encore pour l'utilisation de traceurs en lignes lorsqu'ils ne sont pas strictement nécessaires au service demandé par l'utilisateur (article 82 de la loi « Informatique et Libertés »). Dans un tel cas, le consentement demeure la règle sans qu'il ne soit nécessaire de suivre le cheminement présenté ci-dessus.

39. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. L'Enseigne assigne une base légale à chacun des traitements qu'elle effectue en sa qualité de Responsable de traitement et adéquate à chaque finalité en se fondant sur les référentiels et la jurisprudence de la CNIL[13].

Ainsi, par exemple selon ces référentiels, la base légale est la suivante :

- **Prospection commerciale** : l'intérêt légitime du Responsable de traitement après mise en balance des intérêts ou le recueil du consentement, selon les deux cas de figures suivants[14] :
    - **En cas de publicité par courrier postal et appel téléphonique**, l'intérêt légitime de l'Enseigne, étant précisé que les personnes doivent, au moment de la Collecte de leur adresse postale et/ou de leur numéro de téléphone, avoir été informées de l'utilisation de leurs données à des fins de prospection et être en mesure de s'opposer à cette utilisation de manière simple et gratuite ;

Mise à jour – Loi n°2025-594 du 30 juin 2025 contre toutes les fraudes aux aides publiques[15].
L'évolution législative vient désormais poser le principe de consentement préalable pour le démarchage téléphonique non sollicité dans de nombreux secteurs, avec une mise en œuvre progressive.

[13] Voir notamment le référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des activités commerciales de la CNIL : https://www.cnil.fr/fr/gestion-commerciale-et-gestion-des-impayes-la-cnil-publie-deux-nouveaux-referentiels
[14] La prospection commerciale par courrier électronique, CNIL, 26 janvier 2022 : https://www.cnil.fr/fr/la-prospection-commerciale-par-courrier-electronique
[15] LOI n° 2025-594 du 30 juin 2025 contre toutes les fraudes aux aides publiques.

A partir du 11 août 2026, le démarchage téléphonique sans consentement préalable sera interdit, sauf lorsque la sollicitation intervient dans le cadre de l'exécution d'un contrat en cours et présente un lien direct avec son objet.

- **En cas de publicité par voie électronique (SMS, mail, etc.)**, deux situations se présentent :
  - Par principe, le consentement préalable des Prospects est requis, au moyen d'une action positive et spécifique prenant la forme d'une case à cocher précédant l'information « *J'accepte que mes informations soient utilisées pour de la prospection commerciale* » ;
  - Par exception, l'intérêt légitime suffit si :
    - D'une part, si la personne prospectée est Client de l'Enseigne et si la prospection concerne des produits ou des services similaires fournis par l'Enseigne, ou
    - D'autre part, si la prospection de l'Enseigne devait poursuivre un but caritatif.
    - En toute hypothèse, le Client garde la possibilité de s'opposer à l'utilisation de ses données, au moment de la Collecte et à tout moment notamment lors de chaque envoi d'un courrier électronique de prospection ;
- Le recueil du consentement est nécessaire pour les Enseignes transmettant les données à leurs partenaires pour des opérations de prospection commerciale par voie électronique, ce qu'elle peut faire par le biais d'une seule et même case à cocher précédant l'information « *J'accepte que mon adresse électronique soit transmise aux partenaires [Lien vers la liste des partenaires] de la société X à des fins de prospection commerciale par courrier électronique » ;*

- **Opérations liées à la vente (commande, livraison, facturation, etc.) :** l'exécution du contrat qui lie la personne concernée à l'Enseigne ;
  Par exemple, l'exploitant d'un site marchand de vente à distance traitera les données de son Client, aux fins de lui livrer le produit commandé à son domicile : ce traitement sera rendu nécessaire par l'exécution du contrat conclu à distance. Il traitera également les données figurant sur la carte de crédit afin d'encaisser le paiement du prix. Si ce même exploitant répond à une demande de devis que lui adresse un prospect, via son site web, il traitera les données de ce dernier à cette fin, opération alors qualifiée d'exécution de mesures précontractuelles prises à la demande du prospect.
- **Connaissance du Client (statistiques[16], mesures de fréquentation, études marketing)** : le recueil du consentement, ou l'intérêt légitime du Responsable de traitement après mise en balance des intérêts, ;

[16] Voir à ce sujet, la position de la CNIL du 19 juillet 2022 sur la présence des caméras dites « intelligentes » ou « augmentées » dans les espaces publics : https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf (4.4.1. « *À titre d'illustrations, peut être considéré comme « statistique » un dispositif permettant de […] comptabiliser les flux de visiteurs pour calculer le tarif d'un bail commercial assis sur*

- **Surveillance du Client** (lutte contre la fraude, vidéoprotection des points de vente physiques) : l'intérêt légitime du Responsable de traitement après mise en balance des intérêts.

40. **Exemples de bases légales usuelles / pertinentes pour les Enseignes**. Au cas particulier, et à titre non exhaustif, l'Enseigne retient les bases légales suivantes qu'elle justifie :

i. L'obligation légale comptable et fiscale qui lui incombe dans le cadre du traitement lié aux déclarations comptables pour lequel, en qualité de commerçant, elle conserve les données de facturation (découlant des documents comptables et pièces justificatives) pendant une durée de dix ans, conformément aux termes de l'article L.123-22 du Code de commerce ;

ii. Le recueil du consentement des internautes dans le cadre de l'utilisation de traceurs en lignes (cookies, identifiants mobiles, etc.) lorsqu'ils ne sont pas strictement nécessaires au service demandé par l'utilisateur (publicité en ligne, etc.). En effet, les cookies dits « techniques » ou « fonctionnels » (par exemple, les cookies pour le panier d'achat ou ceux destinés à l'authentification auprès d'un service, etc.) ne nécessitent pas le consentement des utilisateurs ; leur utilisation peut relever de l'intérêt légitime de l'Enseigne Responsable de traitement ;

PREUVE DU CONSENTEMENT

(b) Cas général

Le responsable du traitement doit être en mesure de démontrer à tout moment et individuellement que la personne a bien consenti, dans des conditions valides.

Pour ce faire, les responsables du traitement doivent documenter les conditions de recueil du consentement. La documentation doit permettre de démontrer :

- La mise en place de mécanismes permettant de ne pas lier le recueil du consentement, notamment à la réalisation d'un contrat (consentement « libre ») ;
- La séparation claire et intelligible des différentes finalités de traitement (consentement « spécifique » ou « granularité du consentement ») ;
- La bonne information des personnes (consentement « éclairé ») ;
- Le caractère positif de l'expression du choix de la personne (consentement « univoque »).

Les responsables du traitement peuvent notamment tenir un registre des consentements, qui peut s'insérer dans la documentation plus générale de l'organisme.

Source : https://www.cnil.fr/fr/les-bases-legales/consentement

la fréquentation. Ce traitement, ***réalisé à partir de l'analyse des images issues des caméras dans le centre commercial, transmet uniquement des informations statistiques sur la fréquentation - par exemple les taux d'hommes et de femmes et ou de personnes ayant entre 25 et 35 ans*** »).

(c) Cas spécial des cookies et autres traceurs

Pour les cookies et autres traceurs, une preuve de procédé est suffisante (voir les délibérations CNIL 2020-091 et 2020-092).

iii. Son intérêt légitime en matière de prospection commerciale non-automatisée (voie postale) dans le cadre du traitement de publicité personnalisée, grâce auquel elle procède à l'envoi de sollicitations personnalisées en sa qualité de Responsable de traitement après réalisation du test de mise en balance des intérêts précité ;

iv. Le recueil du consentement pour la sollicitation par l'Enseigne d'une Personne Concernée dont elle a obtenu les coordonnées par transmission, à des fins de prospection commerciale par voie électronique ;

v. Son intérêt légitime après mise en balance[17], dans le cadre du traitement mis en œuvre par le commerçant à des fins de prévention de la fraude.

41. **EXIGENCE AUDITABLE : ETABLIR L'EXISTENCE D'UNE TRACE ECRITE JUSTIFIANT QU'UNE BASE LEGALE FONDE CHAQUE TRAITEMENT REALISE**. Pour ce faire, l'Enseigne indique dans son Registre des traitements la base légale retenue pour chaque traitement et communique aux personnes concernées les mentions d'informations nécessaires. Cette base légale doit être documentée pour chaque finalité identifiée.

Selon les bases légales, l'Enseigne s'assure :

- Pour le consentement : de la mise en place et l'accessibilité d'un mécanisme de refus et de retrait du consentement aussi simple que l'acceptation.
- Pour l'exécution contractuelle : des documents contractuels (CGV, CGU, etc.) attestant que la personne concernée est partie au contrat.
- Pour l'obligation légale : d'avoir identifié la disposition impérative fondant le traitement.
- Pour l'intérêt légitime : du document contenant le test de mise en balance[18].

L'Enseigne qui n'est pas en mesure de justifier d'une base légale valable s'expose à une procédure de sanction menée par l'organisme de contrôle dans les termes exposés au Chapitre 4 « Gouvernance » du Code.

[17] CNIL, L'intérêt légitime : comment fonder un traitement sur cette base légale ? https://www.cnil.fr/fr/linteret-legitime-comment-fonder-un-traitement-sur-cette-base-legale

[18] Voir notamment le référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des activités commerciales de la CNIL, précité.

ILLUSTRATIONS PRATIQUES

Il peut arriver que l'exploitant étudie le comportement général de ses clients, afin de piloter son activité et améliorer ses offres. Dans ce cas, il poursuit notamment un intérêt de nature commerciale, lequel est réputé légitime[19] sauf à méconnaître les intérêts ou droits fondamentaux desdits clients (appréciation qui doit être faite à l'issue d'un test de mise en balance – motivée et documentée), auquel cas il devra alors recueillir le consentement de la personne.

En cas de prospection commerciale, le commerçant doit distinguer plusieurs cas :
- si la prospection est adressée par voie postale, il peut s'appuyer, en principe, sur l'intérêt légitime ;
- si la prospection est adressée par courrier électronique, alors un texte spécial[20] exige de recueillir le consentement préalablement de la personne concernée, sauf si les conditions cumulatives suivantes sont réunies : (i) les données de la personne ont été collectées directement auprès de la personne, à l'occasion d'une vente, dans le respect du RGPD ; (ii) que la prospection envisagée porte sur des produits qui sont proposées par la même enseigne que celle auprès de laquelle la personne concernée a préalablement acquis un produit et analogue aux produits précédemment acquis ; (iii) la personne se voit donner clairement et expressément la faculté de s'opposer préalablement sans frais et de manière simple à l'utilisation de ses données pour la finalité de prospection commerciale au moment de la collecte et, à tout moment, ultérieurement ;
- si l'enseigne transmet des données à caractère personnel à des partenaires (à savoir, d'autres enseignes commercialisant des produits et services distincts) pour leurs propres opérations de prospection par voie électronique, le consentement préalable des personnes concernées devra être recueilli[21].

2.1.2. Le cas des traitements ultérieurs

42. **RAPPEL DE LA RÈGLE.** L'article 5 du RGPD prévoit que les données à caractère personnel ne peuvent être « *traitées ultérieurement de manière incompatible* » avec les finalités pour lesquelles celles-ci ont été collectées. Lorsque la compatibilité du traitement est établie, celui-ci doit respecter les mêmes exigences applicables au traitement initial dont il est issu.

[19] G29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (page 39)
[20] Article L.34-5 du code des postes et communications électroniques, issu de la transposition de la Directive 2002/58/CE modifiée.
[21] Recommandation CNIL, 27 janvier 2022 « la prospection vers les particuliers (B to C) : quelles règles pour transmettre des données à des partenaires ? : https://www.cnil.fr/fr/la-prospection-vers-les-particuliers-b-c-quelles-regles-pour-transmettre-des-donnees-des-partenaires

- Les traitements usuellement admis comme compatibles pour le secteur

43. **Présomption de compatibilité pour certains traitements**. Les traitements à des fins statistiques, au sens du RGPD, sont usuellement considérés comme compatibles avec les finalités initiales en application de l'article 5, b) du RGPD. Ils bénéficient en effet d'une présomption qui permet de les dispenser de test de compatibilité ci-après développé.

44. **Test de compatibilité**. Autrement, le test de compatibilité en cinq étapes doit être réalisé, sauf Collecte du consentement. Si le consentement n'est pas recueilli, l'exigence de compatibilité nécessite que le traitement ultérieur doive répondre aux critères du test (article 6.4 du RGPD), à défaut duquel il ne pourra être mis en œuvre[22] :

    - Le degré de proximité, correspondant à la capacité que les personnes concernées ont de prévoir le traitement ultérieur ;
    - Le contexte de la collecte initiale, signifiant que la finalité du traitement ultérieur doit s'en déduire facilement ;
    - La nature sensible ou non des données collectées ;
    - Les conséquences ou non dommageables du traitement ultérieur sur les personnes concernées ;
    - Les garanties appropriées, nécessitant de prendre en compte les mesures techniques et organisationnelles adoptées par le Responsable de traitement ultérieur (telles que le chiffrement et l'anonymisation).

45. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. En pratique, les Enseignes qui procèdent à un traitement ultérieur s'engagent à réaliser ce test de compatibilité, c'est-à-dire qu'elles veillent à s'assurer des points suivants :

    - Que le Client livré d'un produit acheté par le canal e-commerce puisse légitimement s'attendre à ce que ses données soient retraitées aux cas de recouvrement de sommes éventuelles qui auraient été bloquées à la suite du paiement en ligne ;
    - Que les données retraitées ne concernent que des données de paiement, strictement nécessaires à la poursuite de la finalité du recouvrement des sommes dues ;
    - Qu'il n'existe aucune conséquence dommageable de ce retraitement pour le Client ;
    - Qu'elle met en place des garanties nécessaires liés à ce traitement ultérieur.

[22] G29 (ancien CEPD), avis 03/2013 du 2 avril 2013.

SUR LA COLLECTE DES DONNEES BANCAIRES

Lors du paiement, le Client va saisir diverses données relatives au paiement, notamment à sa carte bancaire (numéro, date de fin de validité, cryptogramme visuel).

Ces données doivent être traitées avec vigilance.

S'agissant de la base légale, le numéro d'une carte de paiement peut être conservé pour permettre des achats ultérieurs à condition d'avoir recueilli le consentement des Clients à la conservation des données au-delà d'une transaction (l'acceptation des conditions générales d'utilisation ou de vente n'est pas considérée comme ne modalité suffisante de recueil du consentement). Si le numéro de la carte bancaire est conservé pour permettre un paiement échelonné convenu contractuellement, la base légale est celle de l'exécution du contrat.

Toutefois, en cas de souscription du Client à un abonnement « premium », « à volonté » permettant de bénéficier, gratuitement ou non, de services annexes visant à faciliter leurs achats, l'Enseigne pourrait se fonder sur son intérêt légitime. Dans ce cas, elle doit veiller à (i) fournir une information suffisamment complète, visible et explicite, (ii) permettre aux Clients d'exercer facilement leur droit d'opposition, (iii) permettre facilement et à tout moment, sur le site marchand, la suppression des données bancaires, (iv) de tenir compte du refus exprimé par le client s'agissant de la conservation de la carte bancaire et de ne lui proposer par la suite une telle conservation qu'avec son consentement libre, éclairé et spécifique, par exemple, par une case à cocher, et (v) de mettre en œuvre des mesures de sécurité appropriées.

S'agissant des durées de conservation, il est bon de noter que le cryptogramme visuel de la carte bancaire doit systématiquement être supprimé une fois la transaction effectuée.

S'agissant des autres données bancaires (numéro de carte et date d'expiration), leur durée de conservation varie en fonction de la finalité pour laquelle elles sont conservées :

FINALITÉ	DURÉE DE CONSERVATION
Paiement unique	Jusqu'au paiement complet. Jusqu'à la réception du bien ou à l'exécution de la prestation de service. Augmenté du délai de rétractation prévu pour les ventes de biens et fournitures de prestations de services à distance
Abonnement avec tacite reconduction	Jusqu'au terme de la dernière échéance.
Abonnement sans tacite reconduction	Jusqu'au terme du contrat.
Gestion des réclamations	13 mois, suivant la date de débit ou 15 mois en cas de cartes de paiement à débit différé. Les données ainsi conservées à des fins de preuve doivent être conservées en archive intermédiaire et n'être utilisées qu'en cas de contestation de la transaction.

Faciliter les achats ultérieurs	Jusqu'au retrait du consentement et/ou à l'expiration de la validité des données de la carte bancaire
Fourniture de services annexes, dans le cadre d'un abonnement *premium* ou à volonté	Tant que dure la fourniture des services additionnels et jusqu'à l'exercice effectif du droit d'opposition

Source : https://www.cnil.fr/fr/le-paiement-distance-par-carte-bancaire

46. **EXIGENCE AUDITABLE : ETABLIR L'EXISTENCE ET LA VALIDITE D'UN TEST ECRIT DE COMPTABILITE**. Les Enseignes doivent disposer d'une analyse documentée afin de s'assurer de la validité :
    - des finalités initiales (indiquées dans le registre des activités de traitement, la documentation pour l'information des personnes ou l'AIPD) ;
    - et des étapes du test de compatibilité pour procéder au traitement ultérieur réalisé.

ILLUSTRATIONS PRATIQUES

Par exemple, peut être considéré comme compatible le traitement ultérieur poursuivant comme finalité la gestion des paiements et des opérations de recouvrement, effectué à la suite d'une collecte poursuivant comme finalité initiale la livraison de produits achetés en ligne[23].

47. **Le consentement, dispense du test de compatibilité**. Dans l'hypothèse où le traitement ultérieur est fondé sur le consentement de la personne, alors il est naturellement soustrait à l'exigence de compatibilité.

- Les traitements pour lesquels un consentement de la personne est requis

48. **L'exigence de consentement pour la prospection par courrier électronique**. Y compris lorsqu'il s'agit d'un traitement ultérieur, la prospection commerciale par courrier électronique est possible à condition que les personnes aient explicitement donné leur accord pour être démarchées, sauf les cas précédemment exposés (*cf. 2.1.1. Les bases légales admissibles*), au moment de la Collecte de leur adresse électronique.

ILLUSTRATION PRATIQUE

Par exemple, doit être considéré incompatible le traitement ultérieur poursuivant comme finalité l'analyse individuelle des actes d'achat visant à détecter notamment l'état de grossesse au vu de ces achats, effectué à la suite d'une collecte initiale réalisée à l'occasion de la souscription d'une carte de fidélité lors de laquelle il était simplement indiqué qu'elle serait « utilisée à des fins marketing, notamment afin de fournir au client des offres spéciales et des réductions »[24].

[23] G29 (ancien CEPD), avis 03/2013 du 2 avril 2013, précision étant faite que les e-commerçants le prévoient désormais cette finalité dès la conception du traitement initial.
[24] G29 (ancien CEPD), avis 03/2013 du 2 avril 2013, précité.

2.1.3. Le cas des traitements soumis à analyse d'impact relative à la protection des données (AIPD)

49. **RAPPEL DE LA RÈGLE.** Certains traitements, dès lors qu'ils sont susceptibles « *d'engendrer un risque élevé pour les droits et libertés des personnes physiques* » compte-tenu de leur nature, de leur portée, de leur contexte et de leurs finalités, sont soumis à une analyse d'impact, obligation issue de l'article 35 du RGPD. Lorsque l'analyse d'impact révèle un « risque élevé » persistant malgré les mesures envisagées par le responsable de traitement[25], ce dernier est alors dans l'obligation de consulter la CNIL avant de mettre en œuvre le traitement.

50. **Traitements soumis à AIPD : première série d'exemples donnée par le RGPD**. L'article 35.3 du RGPD donne une liste non exhaustive des catégories de traitements devant être soumis à une analyse d'impact préalable, parmi lesquelles il est nécessaire d'en relever deux :

- « *Prise de décision automatisée produisant des effets juridiques ou affectant de manière significative la personne concernée* », mentionné à l'article 22.1. RGPD (« *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ») il s'agit notamment des traitements pouvant aboutir à des exclusions ou à des discriminations. Le G29 vise l'évaluation ou la notation.

- « *Surveillance systématique à grande échelle d'une zone accessible au public* », il s'agit, par exemple, des traitements utilisant les dispositifs de vidéoprotection, ou encore de la localisation (à des fins de ciblage publicitaire ou de mesure d'audience[26], par exemple) déployés sur de vastes zones ouvertes au public (les mesures de fréquentation). Le G29 rappelle que la notion de « traitement à grande échelle » doit être appréciée au regard du nombre de personnes concernées par le traitement, du

[25] RGPD, art. 36.1. Cette disposition doit être interprétée conformément aux utiles précisions du considérant 94 qui indique que le traitement est soumis à analyse d'impact lorsque « *le risque ne peut être atténué par des moyens raisonnables, compte tenu des techniques disponibles et des coûts de mise en œuvre* ». Cette lecture est confortée par le G29 qui, dans ses Lignes directrices du 4 avril 2017, indique que la consultation de l'autorité de contrôle est obligatoire lorsque des « *mesures suffisantes* » ne peuvent pas être trouvées (p. 18).

[26] Pour être plus précis, voici des types de dispositifs pouvant entraîner des traitements de ce type :
- Les dispositifs dits de « *tracking-client* » permettant de savoir combien de passants ont visionné certains panneaux publicitaires en munissant ces derniers de dispositifs vidéo ;
- Les dispositifs dits de et le « *tracking-mobile* » permettant de savoir combien de personnes se sont rendues à l'intérieur d'un magasin en équipant certains espaces de vente de boîtiers captant les données émises par les téléphones portables de leurs visiteurs ; ce type de dispositif peut aussi être utilisé afin de procéder, ensuite, à l'envoi de prospection commerciale personnalisée.
- Les dispositifs dits de « *wifi-tracking* », profitant du fait que certains téléphones se connectent automatiquement sur des réseaux wifi publics, et récoltant à cette occasion de nombreuses informations sur les déplacements des personnes, est également considéré comme une mesure de géolocalisation à des fins publicitaires.

volume de données, de la durée et de l'éventuel caractère permanent du traitement, ainsi que de son extension géographique[27].

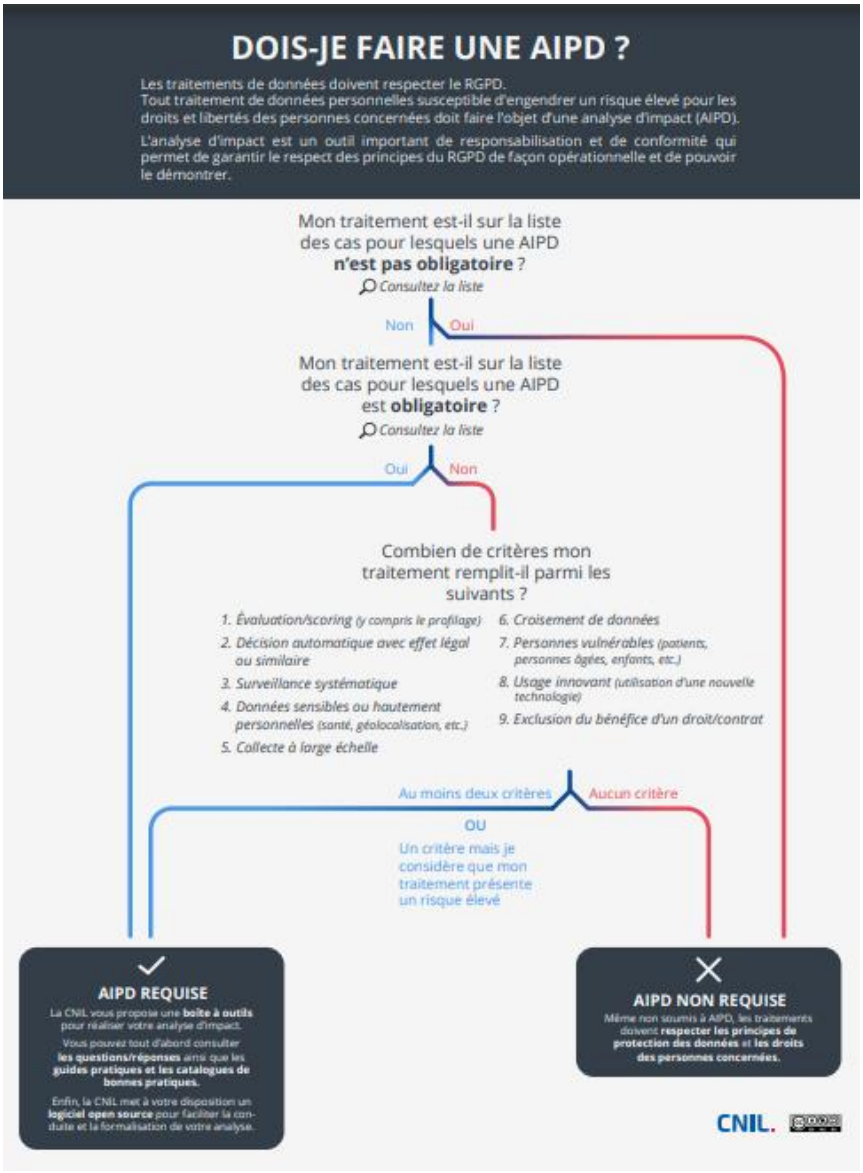
51. **Traitements soumis à AIPD : deuxième série d'exemples donnée par la CNIL**. La délibération CNIL n°2018-327 du 11 octobre 2018 a établi une liste non exhaustive de quatorze traitements obligatoirement soumis à la réalisation préalable d'une analyse d'impact, parmi lesquels figure notamment les « *traitements de données de localisation à grande échelle* ». Elle a adopté une liste des traitements pour lesquels elle estime nécessaire qu'une AIPD soit réalisée[28]. Elle estime qu'une AIPD est notamment requise :

    - Pour les traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci ;
    - Pour les traitements de profilage faisant appels à des données provenant de sources externes.

52. **Traitements soumis à AIPD : les critères donnés par le CEPD**. Cette liste a été établie à partir de celle du Comité Européen à la Protection des Données (ci-après « **CEPD** »), lequel a établi une liste de neuf critères[29] qu'il convient de prendre en compte pour déterminer si le traitement y est ou non soumis du fait des risques qu'il présente pour les droits et libertés des personnes concernées. La nécessité de réaliser une analyse d'impact s'impose dès lors qu'au moins deux des critères suivants sont réunis : évaluation ou notation ; surveillance systématique, données sensibles ou hautement personnel ; traitement à grande échelle ; croisement ou combinaison d'ensemble des données ; caractère vulnérable des personnes concernées ; utilisation innovante ou application de nouvelles technologies ; traitement qui en lui-même empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

53. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. Les Enseignes s'interrogent sur leurs traitements susceptibles d'engendrer la réalisation d'une analyse d'impact en suivant le cheminement suivant :

[27] Lignes directrices adoptées par le G29 (ancien CEPD) le 13 décembre 2016, à propos des DPO.
[28] CNIL, Liste des types de traitement pour lesquelles une AIPD est requise : https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf
[29] Avis du G29 relatif aux analyses d'impact, modifiées et adoptées le 4 octobre 2017.



54. **Le cas de la vidéoprotection et des techniques de suivi commercial, déployées à grande échelle**. Or, les Enseignes disposant d'un réseau étendu de points de vente, au sein desquels circule un nombre important de personnes et dans lesquels peuvent être utilisés des dispositifs de vidéoprotection et de localisation (à des fins de mesure d'audience et/ou de ciblage publicitaire). Il s'agit d'un traitement à grande échelle a *priori* soumis à analyse d'impact obligatoire.

55. **EXIGENCE AUDITABLE : ETABLIR LA NECESSITE DE REALISER UNE/DES AIPD ET SA/LEUR CONFORMITE.** L'Enseigne qui souhaite réaliser une AIPD doit s'assurer, au moyen d'une analyse documentée, de la nécessité de cette AIPD en se fondant notamment sur la base des critères dégagés par le CEPD (visé supra). L'AIPD réalisée pour l'être en utilisant le modèle de son choix ou celui de la CNIL[30], par défaut.

[30] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf

Si l'AIPD se révèle nécessaire, alors l'Enseigne s'engage à ce qu'elle comprenne les informations suivantes :

- Une description systématique des opérations de traitement envisagées et les finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le Responsable de traitement ;
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- Une évaluation des risques sur les droits et libertés des personnes concernées ;
- Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD.

Une fois cette AIPD réalisée, l'Enseigne s'engage à la revoir et à la mettre à jour régulièrement, *a minima* tous les trois ans ; et notamment en cas d'évolution du traitement, des nouvelles technologies ou de nouveaux risques.

ILLUSTRATIONS PRATIQUES

Par exemple, les traitements par lesquels une entreprise établit des profils sur la base des usages ou de la navigation des utilisateurs de son site web.

Par exemple, l'Enseigne qui met en place un dispositif de repérage de fraudeurs dans le cadre de loteries ou de jeux-concours aboutissant à leur refuser le bénéfice d'un gain, procède à du profilage a priori soumis à analyse d'impact préalable.

2.2. Des traitements proportionnés pour le secteur

56. **RAPPEL DE LA RÈGLE.** Tout traitement ne peut porter que sur des données qui sont « *adéquates* », « *pertinentes* » et « *limitées à ce qui est nécessaire au regard des finalités, pour lesquelles elles sont traitées* » aux termes de l'article 5.1 c) du RGPD sur la minimisation des données, et « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* » aux termes de l'article 5.1 e) dudit texte sur la limitation de Conservation.

57. Cette exigence signifie que le Responsable de Traitement doit limiter les caractéristiques de son traitement uniquement à ce qui est indispensable à la poursuite des finalités de celui-ci et pour des durées nécessaires, à défaut desquelles elles seront considérées comme excessives.

2.2.1. La minimisation des données

58. Le choix des données traitées doit être justifié par la finalité du traitement. Autrement dit, ne doivent être collectées que les données strictement nécessaires. A défaut de nécessité, le traitement n'est pas conforme au principe de proportionnalité.

ILLUSTRATIONS PRATIQUES

Par exemple, la société qui conserve des données non nécessaires à l'envoi de la prospection commerciale par mail, en l'occurrence le numéro de téléphone des prospects, commet un manquement au principe de minimisation des données. [31]

59. **TRADUCTION DE LA RÈGLE AU COMMERCE DE DÉTAIL.** Le tableau ci-dessous associe les catégories de finalités visées en Annexe A5 aux sous-catégories de données pertinentes telles qu'évoquées en Annexe A2. Les sous-catégories de données indiquées dans ce tableau ne sauraient valoir autorisation pour les Enseignes de collecter toutes les données qui en découlent. Seules sont possibles celles qui sont rendues strictement nécessaires au traitement cible et à la finalité recherchée. Il est donc rappelé qu'une analyse au cas par cas est nécessaire et doit bien être menée par les Enseignes.

Processus	Finalités (avec, le cas échéant, le détail de celles-ci)	Catégories de données personnelles[32]
Prospection	Publicité ciblée : - Push[33] ; - Display [34]; - Enrichir la base de prospects.	Identité personnelle[35] Identité professionnelle[36] Identifiants uniques[37] Navigation web[38] Situation familiale[39]

[31] CNIL, Délibération du 7 décembre 2020 (SAN – 2020-016) – Décision « PERFORMECLIC »

[32] Dans le présent tableau figure en références de bas de page, une liste purement indicative des types de données correspondant à cette catégorie et pouvant être traitées par l'Enseigne, en lien avec la finalité retranscrite dans ce même tableau. Le choix des types de données relève de la décision souveraine de l'enseigne, et le fait que ces types figurent dans le tableau ne signifie aucunement qu'ils sont systématiquement traités pour la finalité correspondante du tableau.

[33] Voir la définition de ce terme sous le § « 1.4.1 Définitions » supra.

[34] Vor la définition de ce terme sous le § « 1.4.1 Définitions » supra.

[35] Nom, prénom(s) ; date de naissance/âge ; sexe ; langue de communication ; civilité : identifiant quelconque (pseudo, numéro de pseudonymisation) ; adresse électronique personnelle ; numéro de téléphone fixe/mobile personnel.

[36] Numéro SIRET ; numéro professionnel ; adresse électronique professionnelle ; numéro de téléphone professionnel ; adresse postale professionnelle ; numéro de fax.

[37] Identifiant individuel (numéro de client, pseudo, adresse email, empreinte numérique…) ; identifiant technique de l'appareil (adresse MAC [medium access control] IDFA [identifier for advertiser] ; identifiants de navigation (adresse IP, cookie ID, device ID, device Type) ; identifiants uniques (identifiant du réseau mobile SSID [service set identifier], identifiant du réseau filaire [serveur DNS, etc.], identifiant du fournisseur d'accès internet [ISP]).

[38] Recherches effectuées ; liste des sites ou pages consultées (FAI/Entreprise) ; historique des achats ou prestation de service ; historique des produits consultés.

[39] Nombre de personnes composant le foyer et âge des enfants ; situation maritale.

Processus	Finalités (avec, le cas échéant, le détail de celles-ci)	Catégories de données personnelles[32]
	Etude de marché : - Analyser les besoins et les tendances ; - Identifier les nouveaux marchés ; - Mener des expérimentations sur de nouvelles offres.	Habitudes de vie[40] Préférences personnelles[41] Réseaux sociaux[42] Communications[43] Localisation ou Géolocalisation[44] Communications Détails de l'achat[45]
Commerce (vente)	Devis Vente : - Passation de commande ; - Opérations administratives liées aux contrats, aux commandes, aux réceptions, aux factures, aux règlements, à la comptabilité ; - Paiements et factures ; - Prévention de la fraude.	Identité personnelle Identité professionnelle Situation familiale Moyens de paiement[46] Crédit[47] Communications Identité personnelle Identité professionnelle Justificatif d'identité[48] Navigation web Identifiants uniques Moyens de paiement

[40] Présence d'animaux domestiques ; activités sportives/ culturelles ; habitudes alimentaires.

[41] Goûts vestimentaires ; personnalisation de produits.

[42] Personnes suivies ; sujets/ thèmes suivis ; publications réalisées ; réactions postées.

[43] Numéro appelant ; nature de l'appel ; durée ; date et heure de début/fin ; coût ; enregistrement vocal ; messages électroniques, sms, notifications.

[44] Pays, région, ville, code postal ; données GPD ; données GSM ; proximité d'une borne Wifi/Bluetooth placé dans un magasin ou sur un espace extérieur ; déplacements ; enregistrements vidéos.

[45] Numéro de transaction ; produits achetés (données corporelles types taille, poids, pointure, mensurations) ; services ou abonnements souscrits ; quantité ; montant ; modalités de règlement ; remise consentie ; reçu.

[46] Numéro de carte bancaire ; date de fin de validité de la carte bancaire ; cryptogramme visuel ; relevé d'identité postale ou bancaire ; numéro de chèque ; autres moyens de paiement (portefeuille électronique, paiement mobile, carte virtuelle, monnaie virtuelle).

[47] Crédit souscrit ; montant et durée ; nom de l'organisme ; impayés du crédit octroyé et affilié à l'enseigne ; avoirs reçus ; acomptes/ ristournes/ retenues/ oppositions.

[48] Pièce d'identité (numéro de CNI/passeport) ; justificatif de domicile. Ce type de données peut, par exemple, être collecté en cas de paiement par chèque, ou encore en cas de détaxe.

Processus	Finalités (avec, le cas échéant, le détail de celles-ci)	Catégories de données personnelles[32]
	Mesures post-contractuelles (Archivage) - la finalité de l'archivage vise à répondre aux besoins suivants : - Intérêt légitime du responsable de traitement d'avoir à faire valoir ses droits en cas d'éventuelle contestation sur l'opération de vente (non-conformité, défaut de paiement, etc.) ; - Répondre à une éventuelle obligation légale de conservation des informations administratives/ comptables liées à la vente. Exécution – Service après-vente : - Livraison ; - Retouche SAV/ garanties/ retours (échange et remboursement) ; - Recouvrements/ réclamations/ litiges.	Détails de l'achat Communications Identité personnelle Identité professionnelle Identifiants uniques Moyens de paiement Communications
Fidélisation	Fidélisation : - Jeux (concours) ; - Loteries ; - Promotions ciblées ; - Publicités ciblées.	Identité personnelle Identité professionnelle Détails de l'achat Situation familiale Habitudes de vie Préférences personnelles Navigation web Communications
Connaissance client Connaissance prospect	Enquêtes de satisfaction, enquêtes, sondages, tests produits Avis produits et contenus	Identité personnelle Identité professionnelle Détails de l'achat Situation familiale Habitudes de vie Préférences personnelles

Processus	Finalités (avec, le cas échéant, le détail de celles-ci)	Catégories de données personnelles[32]
	Analyses statistiques : - Mesures d'audience (site web) ; - Mesures de fréquentation ; - Statistiques commerciales : - Profilage d'analyse et profilage prédictif.	Navigation web Communications Identifiants uniques Navigation web Habitudes de vie Préférences personnelles Réseaux sociaux Détails de l'achat
Surveillance/ sécurité	Mesures de sécurité et évaluation de risques : - Vidéoprotection des points de vente physique ; - Authentification ; - Détection de connexion frauduleuse ; - Se protéger contre les incidents de sécurité informatique.	Identifiants de connexion[49] Géolocalisation Image

60. **EXIGENCE AUDITABLE : CONTRÔLER LA PROPORTIONNALITE DES DONNES TRAITEES.** L'Enseigne s'engage à ne pas collecter davantage de données que celles strictement nécessaires à la finalité poursuivie et, en toute hypothèse, que celles prévues au tableau ci-dessus. A cet effet, elle met en place une procédure de vérification pour assurer le respect du principe de minimisation des données.

2.2.2. La minimisation des Destinataires

61. **Minimisation des Destinataires**. L'accès aux données doit être limité aux personnes habilitées à accéder aux données en fonction de leurs fonctions au sein de l'organisme, de sorte à empêcher tout détournement des données, au regard de la finalité pour laquelle elles sont traitées. Cette règle signifie que seules les personnes étant habilitées – par leurs fonctions et/ou missions – à intervenir dans le traitement peuvent accéder aux données qui s'y rapportent. Il s'agit, en d'autres termes, de la règle du moindre privilège.

62. **Minimisation des Destinataires.** La minimisation des Destinataires induit des contrôles d'accès appropriés, une restriction des accès physiques et techniques et la tenue d'un journal d'accès régulier. Ces mesures seront abordées exhaustivement dans le cadre de la partie « Obligation de sécurité » du présent Code.

[49] Login (identifiant) et mot de passe.

63. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. Le tableau ci-dessous associe des catégories de finalités visées aux catégories de Destinataires telles qu'évoquées au sein de la boîte à outils tenue à la disposition des Enseignes. Les catégories de Destinataires indiquées dans ce tableau ne sauraient être rendus systématiques. Il est donc rappelé qu'une analyse au cas par cas est nécessaire et doit bien être menée par les Enseignes.

Catégories de finalités	Catégories de Destinataires
Publicité ciblée	Salariés du service concerné (salariés habilités) Prestataires d'infogérance informatique et fournisseurs de solutions Cloud Partenaires commerciaux
Etude de marché	Sociétés du groupe affiliées à l'Enseigne Salariés du service concerné (salariés habilités)
Devis	Salariés du service concerné (salariés habilités) Etablissements financiers
Vente	Salariés du service concerné (salariés habilités) Prestataires d'infogérance informatique et fournisseurs de solutions Cloud Prestataires de services Etablissements financiers
Exécution – Service après-vente	Salariés du service concerné (salarié habilité) Prestataires de transports et livraison Etablissements financiers
Mesures post-contractuelles (Archivage)	Salariés du service concerné (salarié habilité) Prestataires techniques (centres d'archivage papier, hébergeurs d'archives numériques)
Audit, précontentieux et contentieux	Professionnels du droit et du chiffre
Fidélisation (Jeux/concours ; loteries ; promotions ciblées ; publicités ciblées)	Agences de communication Partenaires commerciaux
Enquêtes de satisfaction ; avis produits et contenus	Salariés du service concerné (salarié habilité) Prestataires d'infogérance informatique et fournisseurs de solutions Cloud Prestataires de services Partenaires commerciaux
Analyses statistiques	Prestataires d'infogérance informatique et fournisseurs de solutions Cloud Prestataires de services Agences de communication Partenaires commerciaux
Mesures de sécurité et évaluation de risques	Salariés habilités

Catégories de finalités	Catégories de Destinataires
	Prestataires d'infogérance informatique et fournisseurs de solutions Cloud Prestataires de services

64. **EXIGENCE AUDITABLE : L'ADÉQUATION STRICTE ENTRE LES ATTRIBUTIONS RH ET LES HABILITATIONS D'ACCÈS INFORMATIQUES**.
    - **Pour les accédants internes** : L'Enseigne s'engage à établir une politique stricte de contrôle et de gestion des accès et des habilitations, ainsi qu'à mettre en place un Annuaire d'Accès Informatique (ou « **AAI**[50] »), qui indique notamment les fonctions et droits d'accès pour chaque personne habilitée. Elle vérifie que sa politique d'accès donne aux membres de son personnel, ainsi qu'à ses prestataires, partenaires et clients, les droits informatiques strictement limités aux besoins de leurs fonctions.
    - **Pour les Destinataires externes** : l'Enseigne s'assure de la concordance entre les mentions du registre des traitements et les contrats conclus avec ces tiers.

    En toute hypothèse, et en l'absence de politique expressément élaborée, l'Enseigne est en mesure de justifier que les Accédants et les Destinataires ne sont pas plus nombreux que ce qui est strictement nécessaire.

2.2.3. La limitation de Conservation dans le temps

65. **RAPPEL DE LA RÈGLE.** L'article 5-1 e) du Règlement dispose que les données à caractère personnel doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement […] à des fins statistiques […]* ». Appliqué au secteur du Commerce de détail, ce principe se décline de la manière suivante.

(a) Point départ

66. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL (1).** Selon la qualité de Client ou de Prospect de la Personne Concernée, le point de départ de la durée de Conservation applicable au traitement concerné va varier :

- Dans le cas d'une relation commerciale suivie, le point de départ de la durée de Conservation des données est la date de la fin de la relation – qui peut correspondre à la dernière interaction à l'initiative du Client ;
- Ensuite, dans le cas de la prospection commerciale, à l'égard de Prospects non-Clients du Responsable de traitement, le point de départ du délai de Conservation des données court à compter de leur Collecte par le Responsable de traitement ou du dernier contact émanant du Prospect.

[50] Voir la définition de ce terme sous le § « 1.4.1 Définitions » du présent code.

67. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL (2).** Ce point de départ correspond soit à la fin de la relation commerciale, lorsque cette relation existe et s'échelonne dans le temps ; soit à la date de la Collecte en l'absence d'une telle relation à moins qu'il n'existe un évènement extérieur au Responsable de traitement (le dernier contact volontaire pris par la Personne Concernée en matière de prospection commerciale par exemple). Cette dernière interaction peut être alternativement :

- La dernière commande sur le site ou l'achat en magasin ;
- La dernière connexion au compte client ou au compte fidélité ;
- La dernière communication avec le service client ;
- Le dernier contact émanant d'un Prospect[51]

ILLUSTRATIONS PRATIQUES

Par exemple, s'agissant des prospects, la durée de Conservation mise en place par la société s'agissant des données des prospects, à savoir cinq ans à compter du dernier contact émanant de ceux-ci, excède celle nécessaire au regard des finalités pour lesquelles elles sont traitées. La durée de trois ans apparaît proportionnée au vu de la finalité du traitement. Cette durée répond au souhait de la société de promouvoir, comme tout commerçant, ses produits auprès de ses anciens clients et des personnes ne s'étant pas opposées à la réception de tels messages.

Sur le point de départ du délai de Conservation des données des prospects, les données des prospects permettent à un responsable de traitement d'adresser des messages, par exemple par courrier électronique, à des personnes qui montrent un intérêt pour ses produits ou services. Lorsque le point de départ du délai de Conservation des données est le dernier contact émanant du prospect, il doit s'agir d'un évènement permettant de démontrer l'intérêt de la personne pour le message reçu, tel qu'un clic sur un lien hypertexte contenu dans un courriel. Cependant, la seule ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect, dans la mesure où celui-ci peut être ouvert involontairement du fait des modalités de fonctionnement du logiciel de messagerie utilisé ou par erreur.

La participation d'un prospect à un jeu-concours, constitue un contrat émanant de ce dernier et marque ainsi le point de départ d'une nouvelle durée de trois ans à partir de la fin de la relation commerciale.

(b) Durées de Conservation admissibles pour le secteur

68. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL (3).** L'Enseigne s'engage à formaliser un document répertoriant les durées de conservation de toutes les données traitées dans le cadre de son activité de commerce. Le tableau ci-dessous associe les catégories de finalités

[51] La CNIL précise à cet égard que l'ouverture d'un courriel n'est pas considérée comme un dernier contact émanant du prospect (CNIL, Délibération n° 2021-131 du 23 septembre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales), seul un clic actionné dans un lien inséré dans un courriel est considéré comme le dernier contact.

référencées dans la boîte à outils aux durées de Conservation admissibles et conformes au RGPD. Il convient alors de distinguer la base active de la base intermédiaire :

- La base active contient les données nécessaires aux activités courantes qui peuvent être conservées pendant la durée nécessaire à la réalisation des finalités du Traitement ;
- Les archives intermédiaires contiennent les données (i) devant être conservées pour répondre à une obligation légale ou (ii) qui présentent encore pour les services concernés, un intérêt administratif (obligations issues du code civil, code de la consommation, code de commerce, etc.). C'est notamment l'hypothèse des données conservées à titre probatoire, pour lesquelles les durées de Conservation sont fixées par les règles de prescription applicables.

69. **EXIGENCE AUDITABLE : L'EXISTENCE D'UNE POLITIQUE DE DUREES DE CONSERVATION STRICTEMENT NECESSAIRES.** L'Enseigne s'engage à élaborer une politique de durées de Conservation claire et à mettre en œuvre des mesures destinées à la suppression automatique des données au-delà de la durée expressément prévue au sein de la politique.
    - Elle s'assure que les durées qui y sont renseignées n'excèdent pas celles strictement nécessaires aux traitements liés. Si elle ne dispose d'aucune politique de durées de Conservation, l'Enseigne est en mesure de démontrer que les durées de Conservation mises en œuvre n'excèdent pas celles renseignées au sein du tableau ci-dessous.
    - Elle met en place des mécanismes techniques garantissant la mise en œuvre effective de la limitation des durées de Conservation des données (ex. : paramétrage d'une purge automatique ou manuelle à fréquence déterminée).
    - Elle prévoit des procédures de contrôle internes pour s'assurer du respect de ces durées.

    Les Enseignes prennent acte qu'elles s'exposent à une procédure de sanction, dans l'hypothèse où l'Organisme de contrôle relèverait des délais de Conservation considérés comme excessifs au regard des durées suivantes jugées admissibles :

Processus	Finalités	Durées de Conservation admissibles
Prospection	Publicité ciblée : Push[52] - Par voie électronique (en vue de l'envoi de courriel, SMS, système automatisé de communication électronique sans intervention humaine, etc.), pour des biens ou services qui n'ont pas déjà été achetés par les personnes visées - Par voie postale ou système automatisé d'appels donnant	<u>Conservation base active :</u> Jusqu'au retrait du consentement ou l'exercice du droit d'opposition ou 3 ans à compter du dernier contact des personnes avec l'organisme (l'ouverture d'un courriel de prospection sans aucune autre action ne

[52] Voir la définition de ce terme sous le § « 1.4.1 Définitions » du présent code.

	lieu à intervention humaine et appels téléphoniques	pouvant constituer un point de départ[53])[54].
	Publicité ciblée : Display[55] : - Bannières web ; - Contenus en ligne personnalisés ; Proposer des offres personnalisées.	 <u>Conservation base active</u> – durée de vie des traceurs de 6 mois ou jusqu'au retrait du consentement (Cookies soumis au consentement).
	Devis : établissement d'un devis en vue de la vente Vente : - Passation de commande ; - Opérations administratives liées aux contrats, aux commandes, aux réceptions, aux factures, aux règlements, à la comptabilité ; - Paiements et factures ; - Prévention de la fraude.	- Devis : <u>Conservation base active</u> – Durée nécessaire à l'établissement du devis ou à la préparation de la commande et à son acheminement - Vente : <u>Conservation base active</u> : jusqu'à l'exécution de la dernière opération (livraison, paiement ou retour). <u>Durée d'archivage base intermédiaire</u> – Conservation en archivage intermédiaire pour les durées prévues par les textes imposant une obligation de Conservation (Conservation des factures pendant 10 ans), ou des durées de prescription légale (exemple : durée de 5 ans pour les actions personnelles et mobilières, 10 ans à compter de la mise en circulation du produit pour la

[53] CNIL, Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales et Délibération de la formation restreinte no SAN-2020-016 du 7 décembre 2020 concernant la société PERFORMECLIC

[54] Délibération n° 2021-131 du 23 septembre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales. Au terme de ce délai de trois ans, le Responsable de traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées conformément aux dispositions en vigueur, et notamment celles prévues par le code de commerce, le code civil et le code de la consommation.

[55] Voir la définition de ce terme sous le § « 1.4.1 Définitions » du présent code.

		responsabilité du fait des produits défectueux ; donc Conservation des données relatives à la gestion administrative des contrats – hors RIB – pendant 5 ans à compter de la fin du contrat, par ailleurs Conservation des contrats conclus par voie électronique pendant 10 ans à compter de la fin de la prestation[56])[57].
Commerce (vente)	Exécution – Service après-vente – Réclamations : - Retouche SAV/ garanties/ retours (échange et remboursement) ; Recouvrements/ réclamations/ litiges.	Exécution – Service après-vente – Réclamations : Conservation base active : Durée de la relation contractuelle (incluant la période de garantie contractuelle, le cas échéant)
	Contentieux	**Cas du contentieux[58]** Conservation base active - Les données collectées et traitées dans le cadre de la gestion d'un précontentieux doivent être supprimées dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante. Les données collectées et traitées dans le cadre d'un contentieux doivent quant à elles être supprimées lorsque les voies de recours ordinaires et extraordinaires ne sont plus possibles contre la décision rendue. Durée d'archivage base intermédiaire - A l'expiration de la période de Conservation en base active, les données sont supprimées ou, le cas échéant,

[56] Article D213-2 du code de la consommation.

[57] Voir supra.

[58] La base légale, pour cette finalité, sera l'intérêt légitime.

		conservées en archives intermédiaires (si cette Conservation est proportionnée)[59].
Commerce (vente)	Mesures post-contractuelles (Archivage)	*N/A*
Fidélisation	Fidélisation par sollicitation : - Jeux (concours) ; - Loteries ;	Durée de la relation contractuelle[60](issue de l'opération)
	Fidélisation par opérations commerciales : - Promotions ciblées ; - Publicités ciblées.	Jusqu'au retrait du consentement ou l'exercice du droit d'opposition ou pour une durée de 3 ans à compter de la fin de la relation commerciale[61].
Connaissance client Connaissance prospect	Enquêtes de satisfaction, enquêtes, sondages, tests produits ; Avis produits et contenus ; Analyses statistiques : Mesures d'audience (site web) ; Mesures de fréquentation ; Statistiques commerciales ; Profilage d'analyse et profilage prédictif.	Enquêtes de satisfaction, enquêtes, sondages : - Durée nécessaire pour la réalisation de l'objectif de l'enquête ou jusqu'à l'exercice du droit d'opposition ou le retrait du consentement[62] Tests produits et avis produits et contenus : - Durée nécessaire pour la réalisation de l'objectif de l'étude ou jusqu'à l'exercice du droit d'opposition ou le retrait du consentement

[59] Délibération CNIL n° 2016-005 du 14 janvier 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues.

[60] Voir notamment le référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des activités commerciales de la CNIL : https://www.cnil.fr/fr/gestion-commerciale-et-gestion-des-impayes-la-cnil-publie-deux-nouveaux-referentiels

[61] Cette « *relation commerciale* » peut être entendue comme :

- Si la personne concernée est un client, l'expiration du dernier effet du contrat (l'expiration d'une garantie par exemple ;
- Si la personne concernée est un prospect non-client, son dernier contact pris avec le responsable de traitement (Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales, p. 11 : https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf).

[62] Voir notamment le référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des activités commerciales de la CNIL, précité.

		Statistiques de vente : - Durée nécessaire pour la réalisation de l'objectif visé par les statistiques ou jusqu'à l'exercice du droit d'opposition **Cookies** - Conservation base active – durée de vie des traceurs de 6 mois (Cookies soumis au consentement) et 13 mois (Cookies non soumis au consentement, ex. : mesure d'audience des sites et applications mobiles) et durée de vie des informations collectées par l'intermédiaire de ces traceurs de 25 mois maximum pour les traceurs exemptés pour la mesure de l'audience. Les durées de vie mentionnées ci-dessus font l'objet d'un réexamen périodique afin d'être limitées au strict nécessaire.
Surveillance/ sécurité	Mesures de sécurité et évaluation de risques : - Vidéosurveillance ; - Vidéo-protection des points de vente physique ; - Authentification ; - Détection de connexion frauduleuse ; - Se protéger contre les incidents de sécurité informatique.	Enregistrement des traces de connexion - Conservation base active – Un an à compter de la Collecte[63] Contrôle des accès - Conservation base active – 3 mois[64] Image – 1 mois (CNIL)[65]
Respect d'obligations légales	Exercice des droits	**Justificatif d'identité si nécessaire –** La pièce d'identité est conservée le temps nécessaire à la vérification de l'identité de la personne concernée. Toutefois, il est possible de la conserver à des fins de preuves dans des cas exceptionnels où le

[63] Articles L.34-1 alinéa 4 et R.10-13 du CPCE pour les Enseignes qui offrent à leurs Visiteurs un accès à un réseau local, par exemple via un wifi ; https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations ; CJUE, 15 septembre 2016 aff. C-484/14 Tobias Mc Fadden c/ Sony Music Entertainment Germany GmbH

[64] CNIL, L'accès aux locaux et le contrôle des horaires sur le lieu de travail : https://www.cnil.fr/fr/lacces-aux-locaux-et-le-controle-des-horaires-sur-le-lieu-de-travail

[65] CNIL, La vidéosurveillance – vidéoprotection au travail : https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail

		responsable de traitement identifie un risque contentieux fort, selon une analyse au cas par cas et dument documentée. Dans cette hypothèse, la durée de conservation est déterminée selon les délais de prescription de l'action publique prévus aux articles 8 et 9 du Code de procédure pénale.

70. **Exemple**. A titre d'exemple, dans le secteur du Commerce de détail, les Enseignes s'engagent à conserver les données Clients le temps nécessaire à l'établissement d'un devis, à la préparation d'une commande ou à son acheminement. En conséquence, une fois le produit livré, les Enseignes s'engagent à archiver ces mêmes données Clients en base intermédiaire, cette fois, afin de leur permettre de remplir leurs obligations légales en matière comptable et fiscale notamment.
    Les Enseignes peuvent en outre prévoir le paramétrage d'une purge automatique ou manuelle réalisée à une fréquence déterminée permettant la suppression automatique des données au-delà des durées de conservation prévues dans leur politique.

CHAPITRE 3 – LES OBLIGATIONS

3.1. Information des personnes concernées
3.1.1. L'obligation d'information en cas de Collecte directe
3.1.2. L'obligation d'information en cas de Collecte indirecte
3.1.3. Les exceptions à l'obligation d'information

3.2. Procédures d'exercice des droits des personnes concernées
3.2.1. La communication des procédures d'exercices des droits aux personnes concernées
3.2.2. La formalisation d'une procédure interne de gestion des demandes d'exercice des droits

3.3. Encadrement des contrats entre acteurs de traitement
3.3.1. Rappel pédagogique
3.3.2. Application pratique pour qualifier les acteurs de traitement

3.4. Encadrement des Transferts de Données Personnelles en dehors de l'Union européenne
3.4.1. Les pays bénéficiant d'une décision d'adéquation
3.4.2. La démarche à suivre en cas de Transferts de Données Personnelles vers des pays reconnus non adéquats

3.5. Obligation de sécurité
3.5.1. La mise en œuvre de mesures appropriées
3.5.2. Notification en cas de violation de données

3.6. Registre des traitements

3.7. Délégué à la protection des données personnelles (DPO)
3.7.1. Les cas de désignation obligatoire d'un DPO
3.7.2. Les modalités de désignation
3.7.3. Les missions du DPO

3.1. Information des personnes concernées

3.1.1. L'obligation d'information en cas de Collecte directe
3.1.2. L'obligation d'information en cas de Collecte indirecte
3.1.3. Les exceptions à l'obligation d'information

71. **Rappel pédagogique**. Au titre des principes de loyauté et de transparence auxquels elle est soumise en vertu de l'article 5.1. a) du RGPD, l'Enseigne Responsable de traitement doit communiquer aux personnes concernées des informations sur les caractéristiques essentielles des traitements réalisés (ci-après « **Information** »).

72. L'Information doit être rédigée de la manière la plus claire, précise, accessible et simple possible.

3.1.1. L'obligation d'information en cas de Collecte directe

73. **La notion de « Collecte directe ».** La Collecte directe correspond à la situation au cours de laquelle l'Enseigne Responsable de traitement recueille les données auprès de la Personne Concernée, sans intermédiaire, et au moyen d'un dispositif quelconque. Ainsi, par exemple, constitue une Collecte directe celle effectuée au moyen d'un questionnaire, d'une caméra, d'un témoin de connexion – aussi appelé cookie – ou encore d'un panneau publicitaire connecté mesurant la fréquentation. A ce titre, dans un arrêt rendu le 8 février 2017 (n° 393714), le Conseil d'État a précisé que la Collecte de données de passants sur la voie publique, au moyen de panneaux publicitaires munis de capteurs Wi-Fi, constituait une Collecte directe (« *alors même que cette collecte ne nécessite aucune intervention des personnes concernées, elle a néanmoins le caractère direct* »).

74. **RAPPEL DE LA RÈGLE**. Les informations mentionnées à l'article 13 du RGPD – à savoir : a) identité et coordonnées de l'organisme ; b) finalités ; c) base légale du traitement des données ; d) caractère obligatoire ou facultatif de la fourniture des données ; e) Destinataires ou catégories de Destinataires des données ; f) durées de Conservation des données ; g) le cas échéant, le détail des transferts vers des pays tiers (l'existence d'un transfert, les garanties associées et la faculté d'accéder aux documents autorisant le transfert) ; h) droits des personnes concernées ; i) coordonnées du délégué à la protection des données ; j) droit d'introduire une réclamation auprès de la CNIL - doivent être délivrée à la Personne Concernée au plus tard au moment où les données sont collectées. Par ailleurs, en cas de profilage ou de prise de décision automatisée, il convient d'informer les personnes concernées de l'existence de ces dispositifs, sur la logique sous-jacente de ces derniers, ainsi que de l'importance des conséquences prévues de ce traitement pour les personnes concernées (article 22 du RGPD). Si l'information n'a pas été délivrée au moment de la Collecte, alors le traitement ne peut pas être mis en œuvre.

75. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL TRADITIONNEL ET ÉLECTRONIQUE**. L'Information doit être adaptée par les Enseignes aux situations et aux supports de Collecte. Par ailleurs l'Enseigne doit rendre l'ensemble des informations mentionnées ci-après aisément accessibles pour les personnes concernées, sans qu'il soit demandé à ces dernières de faire preuve d'une détermination particulière pour accéder aux informations[66] :

[66] Le bulletin d'adhésion papier au programme de fidélité qui résume les mentions d'information et renvoie sur la page d'accueil du site de la société concernée pour des mentions plus complètes, sans plus de précisions, manque à l'obligation de rendre l'information aisément accessible prévue à l'article 12 du RGPD. Les mentions d'information dissimulées parmi des conditions générales d'utilisation du site internet de la société d'une longueur déraisonnable conduisant l'utilisateur à faire défiler un grand nombre de pages et lire plusieurs dizaines de paragraphes ne sont pas aisément accessibles puisqu'elles demandent aux utilisateurs une détermination particulière pour accéder aux informations sur ces questions (CNIL, Délibération de la formation restreinte n° SAN-2020-008 du 18 novembre 2020 concernant la société CARREFOUR France).

- **L'Information en magasin**. L'Enseigne s'engage à placer un panneau d'affichage dans l'ensemble de ses magasins soumis à vidéo-protection[67] - système soumis à autorisation préfectorale -, afin d'informer les personnes concernées au moyen de panneaux affichés en permanence, de façon visible, et comportant *a minima*, outre le pictogramme d'une caméra indiquant que le lieu est placé sous vidéo-protection : l'identité du responsable du traitement, les finalités du traitement installé ; l'exercice des droits et le droit d'introduire une réclamation auprès de la CNIL. Afin que les panneaux restent lisibles, l'intégralité des informations devant être portée à la connaissance des personnes concernées peut l'être par le biais du site internet, notamment la base légale du traitement, les Destinataires des données.

EXEMPLE DE PANNEAU D'AFFICHAGE STANDARDISE A FIGURER DANS LES MAGASINS DE VENTE PHYSIQUE
« ETABLISSEMENT SOUS SURVEILLANCE VIDEO *Etablissement placé sous vidéoprotection par la société X pour la sécurité des personnes et des biens.* *Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité de la société X et par les forces de l'ordre.* *Pour exercer vos droits Informatique et Libertés, notamment votre droit d'accès aux images qui vous concernent, ou pour toute information sur ce dispositif, vous pouvez contacter notre délégué à la protection des données en écrivant à [email] ou à l'adresse postale [XXX].* *Pour en savoir plus sur la gestion de vos données personnelles et de vos droits, rendez-vous sur la politique de confidentialité disponible sur le site internet de la société.* *Vous pouvez introduire une réclamation auprès de la CNIL sur cnil.fr/plaintes »*

- **L'Information en ligne**.
    - Des mentions allégées. Pour éviter des mentions trop longues, l'Enseigne peut donner un premier niveau d'information en fin de formulaire de contact, comprenant *a minima* :

        - L'identité du responsable du traitement,
        - La finalité (exemples : prospection commerciale, livraison de biens ou de services, statistiques…),
        - Une description des droits des personnes,

Et renvoyer à une politique de confidentialité (ex. par lien hypertexte sur le site internet, ou une annexe sur un formulaire papier).

[67] Article R253-6 du Code de la sécurité intérieur.

PROSPECTION PAR COURRIEL[68] [à faire figurer sur le formulaire de commande][69]

[EXEMPLE DE MENTION POUR LES CLIENTS D'UN SITE DE VENTE EN LIGNE en cas de prospection concernant des produits/services similaires] « Les données personnelles collectées sur le présent formulaire font l'objet d'un traitement réalisé sous la responsabilité de la société X, afin de nous permettre de gérer votre commande.

Nous utilisons également votre adresse électronique afin de vous adresser des publicités concernant des produits analogues à ceux que vous commandez. Si vous ne souhaitez pas recevoir de telles sollicitations, cochez la case ci-dessous :

[Case non pré-cochée] : Je m'oppose à ce que la société X me propose par courriel des produits analogues à ceux que j'ai déjà commandés.

[EXEMPLE DE MENTION (i) POUR LES CLIENTS D'UN SITE DE VENTE EN LIGNE en cas de prospection concernant des produits/services non similaires, (ii) POUR DES PROSPECTS D'UN SITE DE VENTE EN LIGNE] Si vous consentez à nous permettre d'utiliser votre adresse électronique afin de vous adresser des publicités concernant des produits autres que ceux que vous commandez, nous vous remercions de cocher la case ci-dessus :

« ☐ J'accepte que mes informations soient utilisées pour de la prospection commerciale par courriel ».

Outre le droit de porter réclamation devant la CNIL, vous disposez d'un droit d'accès, de rectification et, le cas échéant, d'un droit à la portabilité et à l'effacement de vos données, ainsi que d'opposition aux traitements ou à leur limitation et, enfin, du droit de définir des directives post-mortem.

*Pour en savoir plus consultez notre politique de gestion des données, en cliquant **ici**. »*

- La politique de confidentialité. En complément des mentions allégées précitées (informations de premier niveau recommandées par la CNIL) sur le formulaire de Collecte, L'Enseigne Responsable de traitement s'engage à insérer, pour les Visiteurs et les Utilisateurs qui consultent le site internet, l'ensemble des informations requises par le RGPD au sein de la politique de confidentialité

[68] CNIL, Exemple d'information clients d'un site de vente en ligne (prospection par courriel et transmission de données à des partenaires commerciaux) : https://www.cnil.fr/fr/exemple-dinformation-clients-dun-site-de-vente-en-ligne-prospection-par-courriel-et-transmission-de

[69] Cette mention est à adapter au cas par cas, étant précisé qu'il est loisible aux Enseignes d'insérer une mention plus allégée notamment dans l'information de l'existence des droits en mentionnant, par exemple : « *Outre le droit de porter réclamation devant la CNIL, vous disposez de droits dont le détail est exposé au sein de la politique de confidentialité* »

disponible sur son site Internet. A titre d'exemples, dans sa politique de confidentialité (voir **Annexe B** pour un modèle), l'Enseigne :

- Indique la base légale appropriée claire et précise pour chacun des traitements qu'elle met en œuvre et chaque finalité[70] [71] ;
- Informe précisément les personnes concernées des catégories de Destinataires des données[72].

- **Les Cookies et autres traceurs concernant l'information des Visiteurs et des Utilisateurs :** Pour rappel, un cookie est un petit fichier informatique, un traceur, déposé et lu par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé (ordinateur, smartphone, liseuse numérique, console de jeux vidéo connectée à Internet, etc.). L'Enseigne s'assure que les personnes concernées soient clairement informées de l'identité du Responsable de traitement, des finalités des traceurs avant de consentir, de l'existence d'une possibilité de retirer son consentement, des conséquences qui s'attachent à une acceptation ou un refus de traceurs, de l'identité de tous les acteurs utilisant des traceurs soumis au consentement[73]. Par ailleurs, s'agissant des modalités

[70] La société, qui met en œuvre plusieurs traitements, et qui indique que la lutte contre la fraude ou encore ceux mis en œuvre dans le cadre des achats effectués sur le site web de la société reposent sur le consentement des personnes dès lors que cette base légale est plus protectrice, alors que la base légale appropriée doit reposer soit sur le contrat, soit sur les intérêts légitimes poursuivis par cette dernière, contrevient à l'obligation d'information des personnes concernées, qui exige que la base légale du traitement soit claire et précise *(*CNIL, Délibération du 28 juillet 2020 (SAN – 2020-003) – Décision « SPARTOO »).

[71] La société, qui s'abstient d'indiquer, pour chaque traitement mis en œuvre, la base légale correspondante au sein de sa politique de confidentialité, manque à ses obligations *(*CNIL, Délibération du 28 juillet 2020 (SAN – 2020-003) – Décision « SPARTOO ») ; une politique de confidentialité qui omet de mentionner l'information relative aux durées de conservation des données à caractère personnel des prospects, ou encore qui ne permet pas aux personnes de savoir, pour chaque traitement, quelle base juridique fonde celui-ci, ni l'intérêt légitime poursuivi par le responsable de traitement lorsqu'un traitement de données à caractère personnel est fondé sur cette base légale n'est pas conforme à l'obligation d'information de l'article 13 du RGPD (CNIL, Délibération de la formation restreinte n°SAN-2020-018 du 8 décembre 2020 concernant la société NESTOR SAS).

[72] La politique de confidentialité qui indique que les données peuvent être transmises à certains partenaires est imprécise, dès lors que si la société n'est pas tenue de fournir l'intégralité des Destinataires des données, elle doit cependant, au moins, informer les personnes des catégories de Destinataires des données (CNIL, Délibération de la formation restreinte n°SAN-2020-018 du 8 décembre 2020 concernant la société NESTOR SAS).

[73] CNIL, recommandations et lignes directrices, 17 septembre 2020 - Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs » et Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.

de recueil du consentement, l'Enseigne fait attention à ce que le consentement des personnes concernées soit donné librement[74], spécifiquement[75], de manière éclairée[76] et univoque[77]. L'Enseigne veille à instaurer, sur son site internet, un bandeau Cookies conforme aux recommandations de la CNIL du 17 septembre 2020, ainsi que proposé à l'exemple de bandeau figurant en **Annexe B** et proposant un lien d'accès direct à la politique de confidentialité / politique Cookies pour davantage de détails. L'utilisation des Cookies par l'Enseigne fait l'objet d'une information – par le biais d'un bandeau et d'une information détaillée dans la politique de confidentialité – étant précisé que l'Enseigne recueille le consentement des personnes concernées pour l'usage des Cookies non strictement fonctionnels et techniques[78]. L'Enseigne veille enfin à prévoir un mécanisme de retrait du consentement au dépôt des Cookies accessible aisément et à tout moment du parcours du Visiteur et de l'Utilisateur, (par exemple, par la présence d'un lien qui permet de réafficher la fenêtre sur tous les pages du site web en haut à droite ou une icône « Cookies » toujours accessible sur l'écran en bas à gauche). En toute hypothèse, le traitement de données mis en œuvre à partir des Cookies est mentionné dans la politique de confidentialité.

[74] La Personne Concernée doit être libre de consentir ou non au traitement. Il est considéré que la Personne Concernée est véritablement libre de consentir dès lors que le fait qu'elle ne consente pas n'a pas d'incidence majeure sur les produits ou les services qui lui sont fournis. En effet, si l'exécution du contrat ou la fourniture de service est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat, le consentement ne pourra pas être donné librement – Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.

[75] Le consentement ne peut être donné globalement *via* l'acceptation des conditions générales d'utilisation, par exemple – Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.

[76] La Personne Concernée doit être exhaustivement informée sur le(s) traitement(s). A minima, cette information comprend : l'identité du ou des responsables de traitement des opérations de lecture ou écriture, la finalité des opérations de lecture ou écriture des données, la manière d'accepter ou de refuser les traceurs, les conséquences qui s'attachent à un refus ou une acceptation des traceurs et l'existence du droit de retirer son consentement – Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.

[77] La Personne Concernée doit manifester son consentement par le biais d'une action positive de la personne, le fait de continuer à naviguer sur un site étant, à titre d'exemple, insuffisant – Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.

[78] A titre d'exemple, le cookie de langue est un cookie fonctionnel, à l'inverse des cookies Facebook ou Google Analytics lesquels sont des cookies soumis à consentement.

76. **EXIGENCE AUDITABLE (1) AFFÉRENTE À L'INFORMATION EN MAGASIN (ARTICLE 13 DU RGPD)**. L'Enseigne s'engage à ce que les lieux physiques de vente soumis à vidéoprotection comprennent bien un panneau d'information conforme aux exigences d'affichage et d'information à destination du public entrant et sortant.
    - Elle s'engage à afficher de façon visible et en permanence les panneaux d'information comprenant *a minima* :
        - Le pictogramme d'une caméra indiquant que le lieu est placé sous vidéoprotection ;
        - L'identité du responsable de traitement ;
        - Les finalités du traitement mis en place ;
        - L'existence du droit d'introduire une réclamation auprès de la CNIL ;
        - Les modalités d'exercice des droits pour les personnes concernées.
    - Elle est en mesure de justifier cette information en la documentant au préalable et au fil des contrôles internes (photos prise sur site, politique interne, rapport de contrôles sur site etc.).

77. **EXIGENCE AUDITABLE (2) AFFÉRENTE À L'INFORMATION EN LIGNE (ARTICLE 13 DU RGPD)**. L'Enseigne s'engage à insérer l'ensemble des mentions de l'article 13 du RGPD au sein de la politique de confidentialité et du formulaire de recueil des données (ex. : formulaire pour la création d'un compte en ligne, formulaire de contact, etc.).
    - Elle les rend aisément accessibles pour les personnes concernées en un clic, sans avoir à chercher l'information ni rencontrer de difficultés à la retrouver, par exemple au moment de la création de compte.
    - Elle s'assure que ces informations soient communiquées de façon claire et précise, avec un vocabulaire simple et adapté aux personnes concernées visées (ex. : phrases courtes, style direct en évitant les termes juridiques ou techniques).
    - Elle précise la base légale pour chaque traitement énuméré (ex. : consentement, obligation légale ou contractuelle, intérêt légitime), les durées de conservation et les catégories de destinataires des données.

78. **EXIGENCE AUDITABLE (3) AFFÉRENTE AUX COOKIES**. L'Enseigne s'engage :

    - À insérer un bandeau Cookies conformes aux recommandations de la CNIL du 17 septembre 2020 ;
    - À ce qu'aucun cookie soumis à consentement n'ait été déposé, sans que la Personne Concernée n'ait, au préalable, pu y consentir formellement ;
    - À insérer **un premier niveau d'information**, permettant à l'Utilisateur ou au Visiteur d'accepter, refuser et/ou paramétrer le consentement donné pour la présence de Cookies non techniques et fonctionnels et contenant *a minima* :
        - L'identité du responsable de traitement,
        - Les finalités du traitement installé,
        - L'exercice des droits des personnes,

- À insérer **un second niveau d'information**, au sein du paramétrage du consentement des Cookies permettant un choix granulaire des finalités pour lesquelles le consentement est demandé et contenant les informations suivantes :
    - La liste des cookies et/ou des partenaires tiers déposant des traceurs ou un lien vers cette liste actualisée,
    - La base légale du traitement,
    - Les finalités détaillées des cookies soumis à consentement,
    - La durée de conservation des cookies et/ou des données associées,
    - Les conséquences du refus,
    - Les droits des personnes,
    - Les coordonnées du DPO ou du contact pour exercer ces droits,
    - Un lien vers la politique de confidentialité complète du site.
- À insérer un **dispositif** sur le site Internet permettant à l'Utilisateur ou au Visiteur de **retirer son consentement** à tout moment, aussi aisément qu'il l'a donné, et que ce mécanisme de retrait soit accessible sur le même écran que celui permettant d'accepter, et s'attache à vérifier que l'ensemble des informations devant être délivrées à la Personne Concernée soient effectivement portées à sa connaissance.

3.1.2. L'obligation d'information en cas de Collecte indirecte

79. **RAPPEL DE LA RÈGLE.** La Collecte indirecte correspond à la situation dans laquelle les données ne sont pas recueillies directement auprès des personnes (exemples : données récupérées auprès de partenaires commerciaux, de data brokers, de sources accessibles au public ou d'autres personnes)).

80. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL.** L'information doit être délivrée, directement en magasin par le biais d'un panneau d'affichage ou en ligne, aux personnes concernées par l'Enseigne Responsable de traitement ultérieur[79] :

    - dans « *un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois* » après la Collecte[80] ;
    - lorsque les données « *doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication avec ladite personne* »[81], et en toute hypothèse dans le mois suivant l'obtention des données ;
    - 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* », et en toute hypothèse dans le mois suivant l'obtention des données.

81. **Une information élargie en cas de « Collecte indirecte ».** Les mentions d'information doivent reprendre celles fournies en cas de Collecte directe, et mentionner, en complément, les catégories de données à caractère personnel concernées, la source d'où proviennent ces

[79] En effet, l'Enseigne, Destinataire des données collectées par un premier Responsable de traitement est qualifiée de Responsable de traitement ultérieur.
[80] Article 14.3 du RGPD.
[81] Article 14.3. b) du RGPD (c'est notamment le cas de la prospection).

données, et, si cela s'avère impossible (notamment parce que plusieurs sources ont été utilisées, des informations générales à ce sujet), une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

82. **EXIGENCE AUDITABLE : REPRODUIRE LES MENTIONS D'INFORMATIONS EXIGEES PAR L'ARTICLES 14 DU RGPD.** De fait, l'Enseigne s'engage :

    1. A ce que le contenu de l'information soit conforme aux exigences posées par l'article 14 du RGPD ;
    2. A ce qu'une procédure ait été mise en œuvre pour que l'information soit bien délivrée aux personnes concernées dans un délai de 1 mois à compter de la collecte des données ;
    3. A ce que cette procédure soit bien respectée en pratique.

3.1.3. Les exceptions à l'obligation d'information

83. **RAPPEL DE LA RÈGLE**. L'obligation d'information ne s'applique pas lorsque :
    - En cas de Collecte directe et indirecte, la Personne Concernée, par essence déjà Cliente, est déjà informée des caractéristiques du traitement.
    - En cas de Collecte indirecte, l'information de la Personne Concernée se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche. Dans ce cas, l'Entité doit évaluer et documenter le caractère disproportionné en mettant en balance ; d'un côté, les efforts qui lui sont demandés pour communiquer les informations à la personne concernée, et de l'autre les effets sur la personne concernée dans le cas où celle-ci ne recevrait pas ces informations[82]. A cet égard, le nombre de personnes concernées, l'ancienneté des données ainsi que les garanties appropriées éventuellement adoptées devraient être prises en considération.

84. **Avertir les personnes de l'exemption d'information**. Néanmoins, il est, en toute hypothèse, nécessaire de délivrer une information générale (par exemple sur le site internet de l'Enseigne).

85. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. Conformément aux lignes directrices WP260[83], ces exemptions doivent être dument justifiées par l'Enseigne Responsable de traitement, qui doit démontrer les facteurs qui l'empêchent effectivement de fournir les informations en question aux personnes concernées. Si, après une certaine période, les facteurs qui ont causé l'impossibilité n'existent plus et qu'il devient possible de fournir les informations aux personnes concernées, alors le Responsable du traitement doit procéder, sans délai, à l'information requise.

86. **EXIGENCE AUDITABLE : JUSTIFIER DES EXEMPTIONS INVOQUÉES.** L'Enseigne s'engage à documenter et être en mesure de justifier les exemptions éventuelles qu'elle invoque notamment leur

[82] Voir en ce sens, le paragraphe 64 (p. 36) des lignes directrices sur la transparence.

[83] Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 (https://www.cnil.fr/sites/default/files/atoms/files/wp260_guidelines-transparence-fr.pdf)

pertinence par rapport au traitement concerné. Elle s'engage également à délivrer une information générale à ce propos (par exemple sur son site internet).

- **En cas de collecte directe**, l'Enseigne démontre que la personne concernée disposait déjà des informations requises.
- **En cas de collecte indirecte**, l'Enseigne qui invoque une exemption à l'obligation d'information doit justifier :
    - d'efforts disproportionnés : l'Enseigne doit formellement évaluer et documenter le caractère disproportionné de l'effort que représenterait l'information des personnes concernées ;
    - d'une communication prévue par un texte légal : l'Enseigne doit documenter l'analyse expliquant comment la disposition légale invoquée lui est effectivement applicable et l'exonère de l'obligation d'information.

3.2. Procédures d'exercice des droits des personnes concernées

3.2.1. La communication des procédures d'exercices des droits aux personnes concernées
3.2.2. La formalisation d'une procédure interne de gestion des demandes d'exercice des droits

87. **RAPPEL DE LA RÈGLE**. Toute Personne Concernée par un traitement dispose de droits qu'elle peut exercer auprès de l'Enseigne Responsable de traitement en application des dispositions des articles 48 et suivants de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles (ci-après « **LIL** »), et 15 et suivants du RGPD.
88. Cette obligation du RGPD concerne les personnes dont les données sont traitées par l'Enseigne en qualité de Responsable de traitement, c'est-à-dire les Abonnés, les Clients, les Fournisseurs, les Prospects, les Tiers parrainé-Filleul, les Vendeurs, les Visiteurs et les Utilisateurs[84].

89. **Les droits à disposition des personnes concernées**. Les personnes concernées disposent d'un droit d'accès[85], d'un droit à la portabilité[86], d'un droit de rectification de leurs données[87], d'un droit d'opposition au traitement[88], d'un droit à l'effacement de leurs données[89], d'un droit

[84] Annexe A2 – Référentiel des catégories de personnes concernées
[85] Articles 49 LIL et 15 RGPD.
[86] Articles 55 LIL et 20 RGPD : « *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :*
a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et
b) le traitement est effectué à l'aide de procédés automatisés. […] »
[87] Articles 50 LIL et 16 RGPD
[88] Articles 56 LIL et 21 RGPD.
[89] Articles 51 LIL et 17.1 RGPD

de donner des directives relatives au sort des données après la mort[90] et du droit de limiter le traitement des données[91].

ILLUSTRATIONS PRATIQUES

Manquement au droit à l'effacement. La Conservation de l'adresse électronique d'une personne qui a fait une demande de suppression de toutes ses données constitue un manquement au droit à l'effacement, nonobstant que cette adresse soit une clef d'entrée – identifiant interne – pour le responsable de traitement. Le responsable de traitement doit, dans cette hypothèse, procéder à la modification de l'architecture de sa base de données, qui s'apparente à un simple choix pratique[92].

Manquements au droit d'opposition. L'insertion d'un lien de désabonnement à la prospection électronique renvoyant vers une page de connexion de compte client constitue un manquement au droit d'opposition[93], car cela excluait de ce droit tous les prospects n'ayant aucun compte de ce type.
Par ailleurs, l'envoi continu de messages de prospection à des personnes ayant actionné la procédure de désinscription ou de désabonnement constitue un manquement au droit d'opposition des personnes concernées[94].

3.2.1. La communication des procédures d'exercices des droits aux personnes concernées

90. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. L'Enseigne, en qualité de Responsable de traitement, offre aux personnes concernées la possibilité de rectifier, d'effacer, de limiter, d'accéder ou d'exercer leur doit à la portabilité (transmission des données dans un format structuré, couramment utilisé et lisible par machine) les Données Client dans le cadre du service ou de concevoir et déployer leurs propres solutions en utilisant le service. Il est à noter que chacun des droits s'appliquent sous certaines conditions – pouvant notamment varier selon la finalité du traitement de données, sa base légale, le motif invoqué ou encore le type de données concernées.

91. **Le délai de réponse imparti à une demande**. L'Enseigne Responsable de traitement dispose d'un délai d'un (1) mois maximum à compter de la réception de la demande, pour fournir à la personne concernée ayant formulé une demande, les informations sur les mesures prises. Ce délai peut être prolongé de deux (2) mois, compte tenu de la complexité et du nombre de

[90] Ce droit a été introduit par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, retranscrite sous l'article 48 LIL.

[92] CNIL, Délibérations SAN 2020-008 et SAN 2020-009 du 18 novembre 2020 concernant la société CARREFOUR France et la société CARREFOUR Banque.
[93] CNIL, Délibérations SAN 2020-008 et SAN 2020-009 du 18 novembre 2020 concernant la société CARREFOUR France et la société CARREFOUR Banque.
[94] CNIL, Délibération SAN 2020-018 du 8 décembre 2020, Décision « NESTOR ».

demandes[95], étant précisé que la personne doit être informée de cette prolongation et de ses motifs dans un délai d'un mois à compter de la réception de la demande d'exercice de droit.

92. **La question de la sollicitation de la carte d'identité**. La sollicitation systématique d'une copie de la carte d'identité est interdite. La CNIL rappelle ainsi que pour justifier de son identité une personne peut simplement fournir son numéro de client ou d'abonnement en plus de son identité et de son adresse ou en exerçant ses droits depuis un compte où la personne s'est préalablement identifiée (identifiant et mot de passe). L'enseigne en qualité de Responsable de traitement ne peut demander une preuve supplémentaire d'identité que si elle a un « doute raisonnable » sur l'identité de la personne concernée. Cette preuve doit être laissée au choix de la personne concernée, cette dernière n'a pas l'obligation de fournir un titre pour justifier de son identité (article 77 du Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

93. **EXIGENCE AUDITABLE (1) : L'EXERCICE DES DROITS EN LIGNE POUR LES VISITEURS ET LES UTILISATEURS**. Afin de faciliter l'exercice des droits par les personnes concernées, l'Enseigne :

    - Propose un formulaire spécifique intitulé « *Exercer vos droits* » accessible sur son site internet à partir, par exemple, de la politique de confidentialité ou *via* tout onglet approprié, et indiquant que le Visiteur, et a *fortiori*, l'Utilisateur, dispose des droits susmentionnés ; ou créé spécifiquement une adresse email qu'elle reproduit dans sa politique de confidentialité au sein de la clause d'exercice des droits prévue à cet effet ;

    - Alternativement, dirige les Clients-Utilisateurs sur leur espace client correspondant à leur compte personnel qui leur permet, via une interface prévue à cet effet, d'exercer leurs droits de manière simple.

94. **EXIGENCE AUDITABLE (2) : L'EXERCICE DES DROITS EN POINTS DE VENTE POUR LES CLIENTS PHYSIQUES SE PRÉSENTANT EN MAGASIN**. Lors d'une vente physique en boutique, afin de faciliter l'exercice des droits par les personnes concernées, l'Enseigne, de manière cumulative :

    - Propose un formulaire papier intitulé « *Exercer vos droits* », que les Clients peuvent remplir directement lors de leur venue en magasin, ou renvoyer ultérieurement par courrier postal ou scan en renseignant l'adresse postale ou électronique pertinente indiquée au sein du formulaire. Conformément à l'article 78 du décret 2019-536 du 20 mai 2019, il est délivré à la Personne Concernée un avis de réception, daté et signé ;

    - Formalise l'information des personnes concernées par un panneau d'information affiché dans l'enceinte du magasin – en caisse par exemple[96] – énonçant que l'exercice des droits qui sont expressément énumérés peut se faire directement *via* son site internet.

[95] Article 12.3. du RGPD.

[96] Ce panneau pouvant être celui utilisé pour l'information des personnes concernées de la mise en place d'un dispositif de vidéoprotection.

95. **EXIGENCE AUDITABLE (3) : LES MODALITÉS D'EXERCICE.** L'Enseigne est en mesure de démontrer qu'elle propose aux personnes concernées, toutes catégories confondues, d'exercer leurs droits par courriel ou courrier, à l'adresse disponible au sein de la politique de confidentialité du site internet, via leur compte personnel et sur place (dans ses magasins)[97]. Elle les informe également que la demande est gratuite et que le format de la demande est libre (courrier postal, télécopie, courrier électronique, demande physique présentée en personne).
L'Enseigne indique que les personnes formulant une demande doivent inclure les informations suivantes dans leur demande :
    - Le nom et le prénom ou le pseudonyme ou l'identifiant unique,
    - La demande précise (demande d'accès ou de rectification par exemple),
    - La date de la demande,
    - La signature,
    - Si la demande est formulée par un représentant légal ou un mandataire[98], elle doit inclure une procuration écrite.

L'Enseigne répond à la demande dans un délai raisonnable, et au maximum dans un délai de trente (30) jours calendaires de sa réception. Dans l'hypothèse où la demande ne satisfait pas aux exigences requises par le RGPD, l'Enseigne répond à la Personne Concernée afin de lui demander de modifier sa demande dans un délai raisonnable. L'Enseigne s'engage enfin à informer la Personne Concernée de la prolongation du délai de réponse (jusqu'à 2 mois) et du motif du report.

3.2.2. La formalisation d'une procédure interne de gestion des demandes d'exercice des droits

96. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL.** Afin de gérer l'exercice du droit d'accès par les personnes concernées notamment, l'Enseigne s'engage à mettre en place un process interne de gestion automatisée afin d'être en mesure de répondre dans les délais aux demandes formulées.

97. En cas d'exercice du droit d'effacement, l'Enseigne répond à cette dernière dans les meilleurs délais afin de lui demander dans quel cas rentre sa demande. En sa qualité de Responsable de traitement, il appartient à l'Enseigne d'identifier le bien-fondé de la demande au regard de l'article 17.1 du RGPD, à défaut seulement, l'Enseigne est en mesure de lui répondre que l'effacement n'est pas dû.

---

[97] Article 78 du Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[98] https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2021-070-recommandation-exercice-droits- mandataire.pdf : Avant tout établissement du mandat – lequel doit expressément préciser son objet et une durée déterminée de sorte que des conditions générales d'utilisation ne suffisent pas – la CNIL rappelle la nécessité de s'assurer que la personne que le mandataire entend représenter est bien titulaire des droits invoqués.

98. **Exemples** :
    - L'Enseigne fait droit à la demande d'effacement de la personne concernée dont les données ne sont pas ou plus nécessaires au regard des objectifs pour lesquels elles ont été initialement collectées ou traitées (exemple : suite à la clôture d'un compte-client, demande d'effacement des données relative au compte) ;
    - L'Enseigne fait droit à une demande d'effacement des données d'un Prospect qui procède au retrait de son consentement à recevoir de la prospection, en décochant la case prévue à cet effet[99], et à condition que ces mêmes données ne servent pas à d'autres finalités fondées sur une base légale valide[100].

99. **EXIGENCE AUDITABLE : ETABLIR L'EXISTENCE D'UNE PROCEDURE INTERNE DE GESTION DES DEMANDES D'EXERCICE DES DROITS**. Afin de traiter de manière efficace les demandes des personnes concernées et de répondre dans les délais imposés par le RGPD, l'Enseigne est en mesure de démontrer qu'elle dispose d'une procédure adaptée à chaque canal d'interaction avec les personnes concernées et de justifier de la procédure interne de gestion des demandes d'exercice, qu'elle documente, et dont elle informe les services internes en charge d'y faire droit (chat, formulaire de contact, postal, en magasin, réseaux sociaux, etc.) et sensibilise le personnel en contact avec les personnes concernées.

100. **La formalisation d'une politique interne de gestion**. L'Alliance du Commerce propose aux Enseignes de définir et formaliser une politique en interne de gestion des demandes d'exercice de droits telle que proposée ci-après, laquelle fera l'objet du contrôle de la part de l'Organisme de contrôle, sans qu'il ne soit lié par les termes reproduits ci-après :

[99] Par ailleurs, dans le cas où l'Enseigne traiterait des données en provenance de tiers (achat/ location de fichiers externes de données), il conviendrait qu'elle mette en place un « fichier repoussoir » permettant au tiers de l'informer des personnes ayant exercé leur droit d'opposition, de sorte qu'elle le prenne en compte et n'adresse plus de prospection auxdites personnes. Selon les recommandations de la CNIL, ce « fichier repoussoir » ne devrait pas être utilisé à d'autres fins que la gestion du droit d'opposition et seules les données nécessaires devraient y être conservées pour une durée minimum de 3 ans (cf. Comment utiliser une liste repoussoir pour respecter l'opposition à la prospection commerciale ? | CNIL).

[100] A ce titre, il convient de préciser que s'il est possible de conserver dans une même base de données, les données utilisées pour la prospection afin de les utiliser pour d'autres finalité – sous réserve de respecter la nécessité de conserver ces données et de disposer d'une base légale valide pour le traitement – des mesures techniques et organisationnelles doivent être mises en place afin de bien respecter l'effectivité du droit d'opposition ou du retrait du consentement. A titre d'exemple, les personnes qui gèrent les opérations de prospection, ne doivent plus pouvoir transmettre de publicité aux personnes qui se sont opposées ou qui ont retiré leur consentement. Dans tous les cas, il est préférable de recourir à des bases de données distinctes pour les traitements liés à la prospection et les autres traitements, afin d'être certains de respecter le droit d'opposition des personnes concernées.

EXEMPLES DE BONNES PRATIQUES

- ***Droit d'accès*** *: le service client réceptionne la demande, et requiert une preuve d'identité, le cas échéant (uniquement s'il existe un doute raisonnable sur l'identité de la personne concernée et auquel cas celle-ci devra être immédiatement supprimée après consultation), ensuite, il demande au responsable produit d'identifier les données concernées et de les confirmer auprès de l'administrateur IT, et en informe le contact à la protection des données. L'administrateur IT communique l'information au service client, afin de mettre ce dernier en mesure de répondre au client.*

Exemple de réponse à une demande d'accès :

« Chère Madame/Cher Monsieur [Nom]

Nous faisons référence à votre [courrier / lettre recommandée / télécopie / courrier électronique / demande délivrée en main propre] du [date] dans laquelle/lequel vous demandiez à [accéder] aux données à caractère personnel vous concernant que nous détenons.

En réponse à votre demande, nous vous confirmons que nous traitons des données à caractère personnel vous concernant. Ces données portent sur [catégories de données détenues]. Vous trouverez ci-joint une copie conformément à l'article 15.3. du RGPD, des données à caractère personnel détenues dans ce dossier.

Ces données sont issues du traitement [nom du traitement] au titre duquel [nom de l'Enseigne] agit en qualité de responsable du traitement. Le traitement a pour finalité de [décrire les finalités].

Vos données à caractère personnel sont mises à disposition de [catégories de Destinataires – lister autant que faire se peut les Destinataires connus[101]].

[En cas de collecte indirecte uniquement] – Vos données nous ont été communiquées par [source des données].

Vos données sont traitées pour [durée].

Vous avez le droit de demander la rectification, l'effacement, la limitation, l'opposition de vos données à caractère personnel, ainsi que d'introduire une réclamation auprès de la CNIL dans le cas où nous ne respecterions pas votre demande d'accès, de rectification ou d'exercice d'autres droits en vertu de la législation relative à la protection des données.

[101] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62021CC0154 Question préjudicielle du 9 juin 2022 – Affaire C-154/21 RW contre Österreichische Post AG sur la question de savoir si l'article 15 du RGPD signifie qu'il peut être donné la faveur à la liste des catégories de Destinataires (facilitant la réponse du responsable de traitement) ou, au choix et en faveur de la Personne Concernée, aux noms des Destinataires connus.

Nous espérons que la présente réponse à votre demande vous donnera entière satisfaction. Nous restons à votre disposition pour de plus amples informations.

(Formule de politesse) ».

- ***<u>Droit de rectification</u>** : le service client réceptionne la demande, et, le cas échéant, requiert une preuve d'identité (doute raisonnable), ensuite, il transmet au responsable produit qui, lui-même, transfère à l'administrateur IT, et en informe le contact à la protection des données. L'administrateur IT modifie les données et confirme la modification au service client, afin qu'il réponde au client.*

<u>Exemple de réponse à une demande de rectification :</u>

« Chère Madame/Cher Monsieur [Nom]

Nous faisons référence à votre [courrier / lettre recommandée / télécopie / courrier électronique / demande délivrée en main propre] du [date] dans laquelle/lequel vous demandiez à rectifier les données à caractère personnel vous concernant que nous détenons.

En réponse à votre demande, nous vous confirmons avoir rectifié ces données tel que vous nous l'avez demandé.

Nous espérons que la présente réponse à votre demande vous donnera entière satisfaction. Nous restons à votre disposition si nécessaire.

(Formule de politesse) ».

- ***<u>Droit d'effacement / d'opposition / de limitation</u>** : le service client réceptionne la demande, et, le cas échéant, requiert une preuve d'identité (doute raisonnable). Il transmet au responsable produit qui, lui-même, transfère à l'administrateur IT, et en informe le contact à la protection des données. L'administrateur IT efface/restreint, prend acte de l'opposition sur les données et confirme l'opération au service client (et en informe le responsable produit), afin qu'il réponde au client.*

<u>Exemple de réponse à une demande d'effacement / d'opposition / de limitation :</u>

« Chère Madame/Cher Monsieur [Nom]

Nous faisons référence à votre [courrier / lettre recommandée / télécopie / courrier électronique / demande remise en main propre] du [date] dans laquelle/lequel vous nous demandiez [l'effacement des données à caractère personnel vous concernant / d'exercer votre droit de vous opposer au traitement des données à caractère personnel vous concernant / la limitation du traitement des données à caractère personnel vous concernant] que nous détenons.

En réponse à votre demande, nous vous informons que nous avons [effacé vos données à caractère personnel / accepté votre opposition au traitement de vos données / accepté la limitation du traitement de vos données] tel que vous nous l'avez demandé.

Nous espérons que la présente réponse à votre demande vous donnera entière satisfaction. Nous restons à votre disposition pour de plus amples informations.

(Formule de politesse) »

- ***Droit à la portabilité*** : *le client formule sa demande auprès du service client qui la communique au responsable produit qui, lui-même, la transfère à l'administrateur IT, et en informe le contact à la protection des données. L'administrateur IT communique les données au service client qui les communique à son tour au client.*

Exemple de réponse à une demande de portabilité :

« Chère Madame/Cher Monsieur [Nom]

Nous faisons référence à votre [courrier / lettre recommandée / télécopie / courrier électronique / demande délivrée en main propre] du [date] dans laquelle/lequel vous demandiez une copie des données à caractère personnel que vous nous avez fournies.

En réponse à votre demande, vous trouverez ci-joint un fichier au format structuré [à compléter] contenant vos données à caractère personnel.

Nous espérons que la présente réponse à votre demande vous donnera entière satisfaction. Nous restons à votre disposition pour de plus amples informations.

(Formule de politesse) »

101. **EXIGENCE AUDITABLE : ETABLIR LA PREUVE D'UNE RÉPONSE À TOUTES LES DEMANDES**. L'Enseigne s'engage à répondre à toute demande transmise dans un délai raisonnable et au maximum sous trente (30) jours à compter de la réception de la demande, y compris si elle ne détient aucune donnée à caractère personnel.

EXEMPLE DE BONNE PRATIQUE

Exemple de réponse :
« Chère Madame/Cher Monsieur [Nom],

Nous faisons référence à votre [courrier / lettre recommandée / télécopie / courrier électronique / demande délivrée en main propre] du [date] dans laquelle/lequel vous demandiez à [accéder aux/rectifier les] données à caractère personnel vous concernant que nous détenons.

En réponse à votre demande, nous vous informons par la présente que [nom de l'Enseigne] ne détient aucune donnée à caractère personnel vous concernant.

(Formule de politesse) »

3.3. Encadrement des contrats entre acteurs de traitement

3.3.1. Rappel pédagogique
3.3.2. Application pratique pour qualifier les acteurs de traitement

3.3.1. Rappel pédagogique

102. Afin de pouvoir correctement encadrer les contrats, chaque Enseigne doit qualifier les traitements pour lesquels elle agit en qualité de Responsable de traitement, de Sous-traitant ou de Responsable Conjoint de traitement.

103. **Le Sous-traitant : celui qui exécute**. Le RGPD définit le « Sous-traitant » 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* » (Article 4, 8) du RGPD)[102]. Le Sous-traitant ne traite ainsi pas les Données détenues par le Responsable de traitement pour son propre compte[103].

104. **Une qualification devant refléter la réalité opérationnelle**. L'exercice de qualification doit se fonder davantage sur la réalité opérationnelle, que sur les clauses contractuelles ou la qualification juridique choisie par les parties qui ne sont pas déterminantes[104]. Sur un plan pratique, la finalité correspond à l'objectif du traitement (le pourquoi), et les moyens correspondent au comment du traitement. Le CEPD et la CNIL distinguent les moyens essentiels (le type de données à caractère personnel traité, la durée du traitement, les catégories de Destinataires, et les catégories de personnes concernées)[105], le Responsable de traitement doit avoir exercé un contrôle décisionnel sur les finalités et le moyens essentiels du traitement (et pas nécessairement sur les moyens non essentiels, tel que le choix d'un type particulier du matériel et du logiciel, ou encore les mesures de sécurité, qui peuvent être laissés à la discrétion du Sous-traitant).

[102] La condition de « pour le compte du Responsable de traitement » se rapproche de la notion de « mandat » et signifie que le Sous-traitant doit rigoureusement obéir et se limiter aux instructions du Responsable de traitement : à défaut de s'y conformer, le Sous-traitant deviendrait Responsable Conjoint de traitement à côté du Responsable de traitement (G29, avis 1/2010 du 16 février 2010, p.27).

[103] Guidelines du CEPD de septembre 2020, page 18, point 53, and point 79 page 25.

[104] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, *2) Contrôle découlant d'une influence factuelle*, p.14 (§28).

[105] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p.17 (§40)

105. **Contrat(s) de sous-traitance**. L'article 28.3 du RGPD impose à tout Responsable de traitement faisant appel à un Sous-traitant à signer avec ce dernier un contrat, comportant une série de clauses obligatoires[106]. Bien que les décisions relatives à des moyens non essentiels puissent être laissés à la discrétion du Sous-traitant, le responsable du traitement doit donc toujours stipuler les moyens essentiels du traitement dans son accord de sous-traitance.

106. **Contrat(s) entre Responsables conjoints de traitement**. Les Responsables Conjoints de traitement déterminent ensemble les finalités et les moyens du traitement. Dès lors, pour apprécier l'existence de responsables conjoints du traitement, il convient d'examiner si la détermination des finalités et des moyens qui caractérisent un responsable du traitement est décidée par plus d'une partie. Conformément à l'article 26 du RGPD, ils doivent définir contractuellement « *leurs obligations respectives* » afin d'assurer le respect du RGPD, notamment concernant l'exercice des droits des personnes concernées, ainsi que l'accomplissement des obligations d'information des articles 13 et 14 à leur égard[107].

---

[106] Article 28.3 du RGPD : « *Le traitement par un Sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :*
a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le Sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;
b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
c) prend toutes les mesures requises en vertu de l'article 32 ;
d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ;
e) tient compte de la nature du traitement, 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 ;
f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du Sous-traitant ;
g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et
h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.
En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données. »

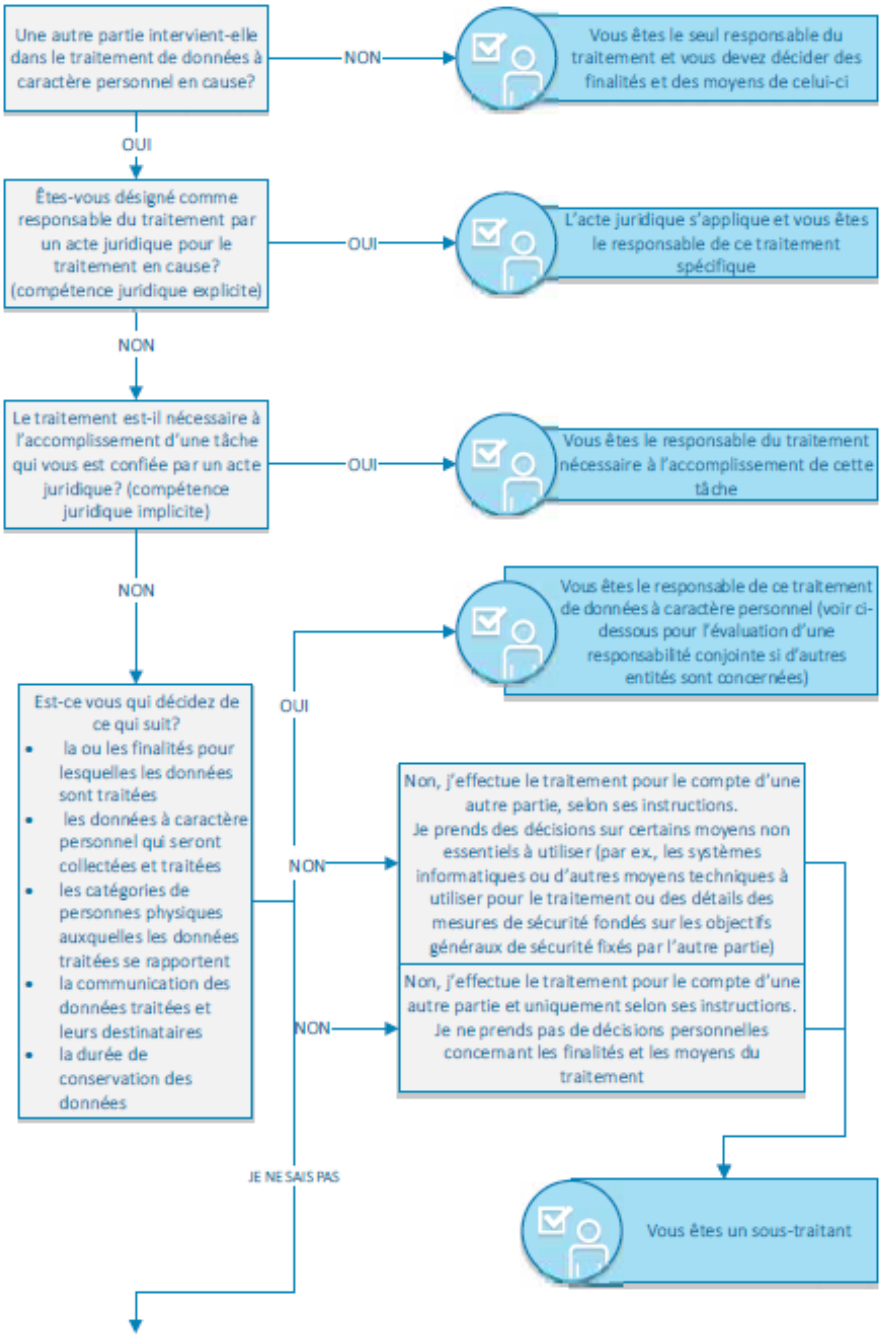
[107] Article 26.1 du RGPD

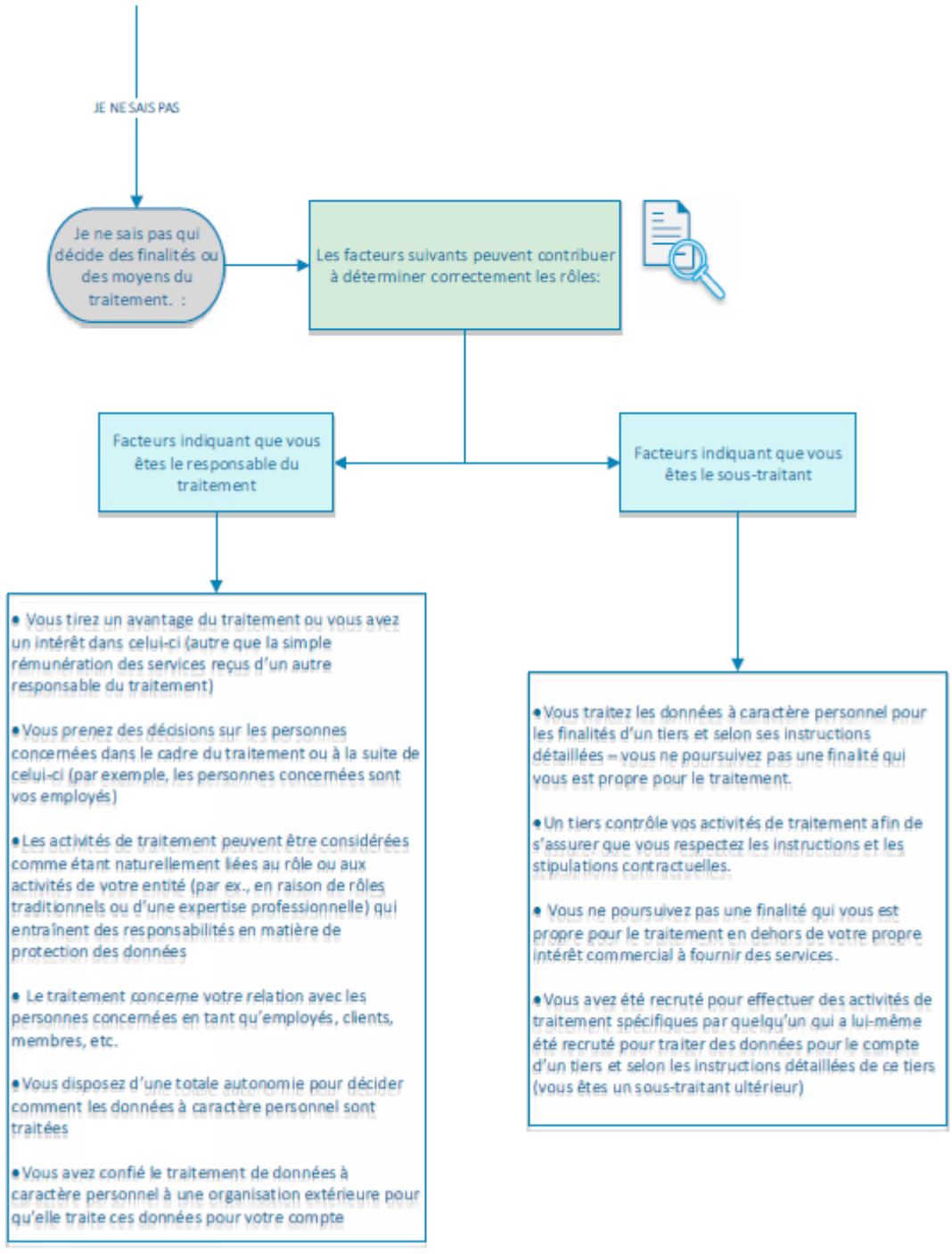
3.3.2. Application pratique pour qualifier les acteurs de traitement

107. **Méthode de qualification**. L'Enseigne devra se conformer à la méthode proposée par le CEPD dans ses Lignes directrices 07/2020 du 7 juillet 2021, actualisées le cas échéant de tout autre texte, dont voici l'annexe 1 reproduite :

Annexe I – Diagramme pour l'application pratique des notions de responsable du traitement, de sous-traitant et de responsables conjoints du traitement

Remarque: afin d'évaluer correctement le rôle de chaque entité concernée, il convient de commencer par identifier le traitement de données à caractère personnel concerné et sa finalité précise. En cas d'entités multiples, il y a lieu d'évaluer si les finalités et les moyens sont déterminés conjointement, ce qui entraîne une responsabilité conjointe.





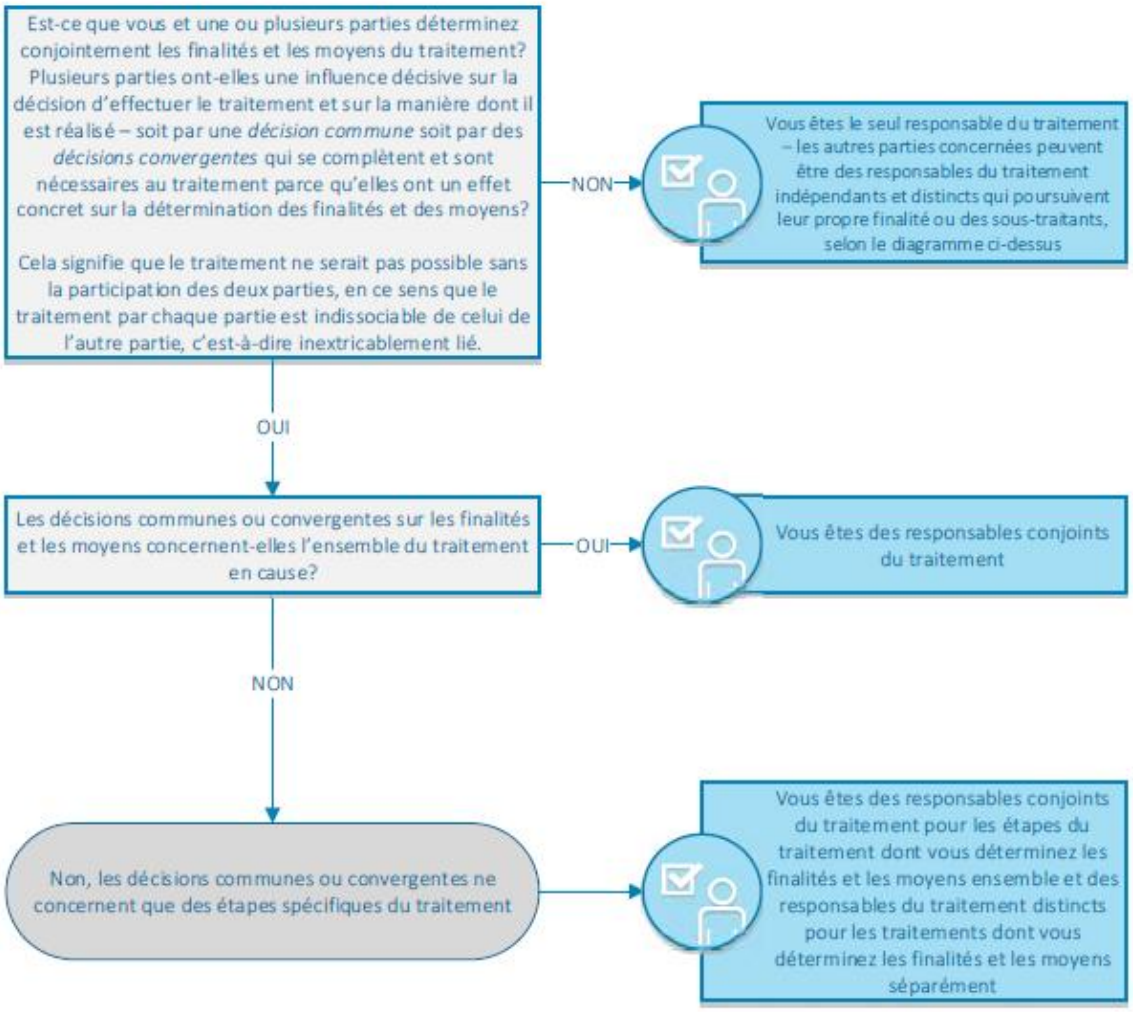
108. **Le critère des instructions**. Concernant les « instructions détaillées » visées dans le schéma ci-dessus, il est indiqué que :

- L'Enseigne, disposant d'un réseau de franchises, qui procède à des campagnes de communication marketing ciblé pour le compte de l'ensemble du réseau – c'est-à-dire qu'elle fait de la prospection par envoi de mails et sms à des clients – est logiquement Responsable du traitement :

    - Car les Enseignes, qui vont collaborer pour relayer l'information, pourraient être qualifiées de responsables conjoints de traitement dans la mesure où elles participent activement à la détermination de la campagne, tandis que si ces dernières agissent davantage comme des exécutants, elles seront alors qualifiables de Sous-traitant ;
    - Néanmoins, la qualification, en fonction de ce critère, est susceptible de varier selon la gouvernance du réseau.
- L'Enseigne, qui recourt à un prestataire d'envoi d'emailings pour réaliser des campagnes, pourrait être qualifiée de Responsable de traitement, tandis que le prestataire pourrait revêtir la qualification de Sous-traitant dès lors que :
    - Son rôle est passif et purement technique, et qu'il agit sur instructions précises de l'Enseigne Responsable de traitement, et/ou
    - Le paramétrage de la solution (mise à disposition de l'Enseigne) est effectué par le client ; si, au contraire, c'est le prestataire qui effectue ce paramétrage, la qualification de responsable (conjoint) de traitement sera à envisagée.

109. **Le critère du contrôle**. Concernant le critère selon lequel « un tiers contrôle vos activités de traitement » visé dans le schéma ci-dessus, il est indiqué que ce contrôle peut s'évaluer par la présence d'une clause d'audit au sein d'un contrat.

Responsabilité conjointe – Vous êtes le responsable du traitement et d'autres parties sont impliquées dans le traitement de données à caractère personnel:



110. **Illustration.** L'Enseigne A (qui commercialise du prêt à porter) s'associe à l'Enseigne B (qui commercialise des chaussures), pour mener avec elle une opération de prospection sur leurs clients respectifs, se matérialisant par un accord de partenariat. Par cette opération, l'Enseigne A fera, auprès de ses clients, la promotion de l'Enseigne B, et réciproquement. Par exemple, pour chaque produit acheté auprès d'une Enseigne, le client de celle-ci bénéficiera d'une réduction lors d'un achat réalisé auprès de l'autre Enseigne.

Cette opération impliquant une utilisation des données à caractère personnel à des fins de prospection partenaire, exigeant un consentement préalable exprès (« *opt'in* »), chaque Enseigne sélectionnera, parmi ses Clients, ceux qui l'ont donné (étape 1 : sélection des clients sollicitables). Ensuite, les messages seront adressés aux clients concernés des deux Enseignes, via un emailing commun créé à cet effet et comportant les deux logos (*co-branding)* (étape 2 : envoi commun). En appliquant la méthodologie

reproduite ci-dessus, il en résulte que :

- Chacune des deux Enseignes intervient dans le traitement de données à caractère personnel en cause au niveau de son étape 2, en ayant déterminé conjointement les finalités (la campagne co-brandée), et les moyens de traitement (notamment, les clients sollicitables et les données concernées à savoir les adresses électroniques), et ce, en vertu d'une décision commune matérialisée par l'accord de partenariat conclu entre les deux Enseignes ;
- Sans l'accord de partenariat précité, ni l'étape 2 du traitement n'aurait pu être réalisée ni l'étape 1 qui y est étroitement liée (aucune des Enseignes n'aurait sélectionné les clients sollicitables pour de la prospection partenaire si un partenariat de prospection n'avait pas été conclu).
- En conséquence, les Enseignes A et B sont responsables conjoints des étapes 1 et 2 du traitement mis en œuvre pour ce partenariat.

111. **En matière de Cookies et traceurs.** Par exemple[108], lorsque des « Cookies » sont déposés par l'Enseigne lors de la navigation des Visiteurs ou Utilisateurs sur son site internet, celle-ci doit être considérée comme Responsable de traitement au sens de la loi. Il en va de même lorsque l'Enseigne sous-traite à des tiers la gestion de Cookies mis en place pour son compte[109] et sur ses instructions. Les autres tiers - prestataires - qui déposent des Cookies à l'occasion de la visite du site d'une Enseigne doivent être considérés comme responsables de traitement. Toutefois, les Enseignes qui autorisent le dépôt et l'utilisation de tels Cookies par des tiers à l'occasion de la visite de leur site doivent également être considérés comme responsables de traitement, alors même qu'ils ne sont pas soumis à l'ensemble des obligations qui s'imposent au tiers qui a émis le cookie, même lorsque ce dernier conserve seul la maitrise du respect de sa finalité ou de sa durée de Conservation[110].

112. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL.** Ainsi qu'il a été préalablement exposé, l'Enseigne, lorsqu'elle agit en qualité de Responsable de traitement, a des obligations légales à respecter. Les obligations de l'Enseigne agissant en qualité de Responsable du traitement sont plus vastes que celles du Sous-traitant ; ce dernier pouvant jouer un rôle de soutien dans l'exécution des obligations du Responsable de traitement. Dans le cadre de l'application du Code, l'Enseigne est qualifiée de Responsable de traitement pour les activités de vente directe ou de réparation auprès des clients personnes concernées, autrement dit pour les traitements liés à la gestion de son activité commerciale, à savoir pour les traitements « activités de base », qui recouvrent son cœur de métier.

113. **Pour l'application des dispositions du Code de conduite**, les Enseignes s'engagent

[108] Il faut considérer que l'Enseigne est toujours impliquée dans la finalité du traitement, la qualification reposant sur celle dépendant des moyens de ce traitement.

[110] Conseil d'Etat, 10ème – 9ème chambres réunies, 06/06/2018, 412589, §11

à mener une analyse précise de qualification des acteurs de traitement[111].

114. **EXIGENCE AUDITABLE (1) : LA BONNE QUALIFICATION DES PARTIES**. L'Enseigne s'engage à procéder à la qualification des acteurs impliqués dans chaque traitement (responsable de traitement, sous-traitants, responsables conjoints etc.) en menant une analyse détaillée écrite, à partir de laquelle elle pourra répartir de manière claire et cohérente les obligations des parties aux différents contrats qui en découlent, conformément aux articles 26 et 28 du RGPD. Elle s'assure que cette qualification n'est pas manifestement erronée.

115. **EXIGENCE AUDITABLE (2) : L'EVALUATION DU CARACTERE SUFFISANT DES GARANTIES FOURNIES PAR LE SOUS-TRAITANT**. L'Enseigne Responsable de traitement s'engage à faire appel à des Sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles de sorte que le traitement concerné garantisse la protection des droits des personnes concernées. A ce titre, l'Enseigne doit se charger d'évaluer ce caractère suffisant des garanties fournies par le Sous-traitant[112]. Pour se faire, elle vérifie :

- La politique en matière de respect de la vie privée, les conditions de service, l'enregistrement des activités de traitement, la politique en matière de gestion des documents, la politique de sécurité de l'information, les rapports des audits externes en matière de protection des données ;
- Les connaissances spécialisées du Sous-traitant (par exemple, l'expertise technique en ce qui concerne les mesures de sécurité et les violations de données), sa fiabilité et ses ressources.

116. **EXIGENCE AUDITABLE (3) : LA VERIFICATION DE LA CONFORMITE DES SOUS-TRAITANTS**. Une fois la qualification réalisée, l'Enseigne s'engage à adopter des clauses contractuelles conformément aux exigences de l'article 28.3 du RGPD, dans le respect de la répartition présentée ci-dessous. L'Enseigne doit réévaluer régulièrement la conformité et la fiabilité de ses sous-traitants via des questionnaires, des audits ou des suivis d'incidents ; et documenter cette évaluation périodique.

OBLIGATIONS DU RESPONSABLE DE	OBLIGATION DU SOUS-TRAITANT (ST)

[111] Cf. 1.4.2. Champ d'application matériel. 28. Dans le cadre de l'application du code, les Enseignes sont qualifiées de Responsable de traitement pour les activités de vente directe ou de réparation auprès du client final. Les Enseignes sont qualifiées de sous-traitant pour les activités pour lesquelles elles agissent en qualité de fournisseurs de service logistique auprès des Vendeurs [*Les Enseignes agissent en qualité de sous-traitant, dès lors qu'elles interviennent dans la chaîne logistique de gestion des stocks, d'envoi des pièces commandées et du service client. L'entité marketplace a la qualité de vendeur et l'Enseigne a la qualité de fournisseur du vendeur. En conséquence, l'Enseigne récupère les données personnelles du client final afin de lui livrer sa commande*]. Dans ce dernier cas, les Enseignes répondront uniquement aux obligations prévues dans le présent Code, qui incombent aux sous-traitants en vertu du RGPD.

[112] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, *1.1. Choix du sous-traitant*, §94 et s.

TRAITEMENT (RT) **(en cas de Responsabilité Conjointe de traitement ces obligations sont réparties dans un contrat)**	
Créer un registre des traitements (comprenant les éléments suivants préalablement définis : des bases légales et des durées de Conservation pour chaque Traitement, les catégories de Données, les finalités du Traitement, les Transferts de Données, etc.)	Créer un registre des traitements comportant uniquement la liste des Traitements effectués pour le compte du RT, les ST ultérieurs, les Transferts éventuels de Données et les mesures de sécurité.
Respecter les principes suivants : - Les Données doivent être collectées pour des finalités déterminées, explicites et légitimes (limitation des finalités) ; - Les Données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation) ; - Les Données doivent être exactes et, si nécessaire, tenues à jour (exactitude) ; Les Données doivent être conservées pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.	
Politique d'archivage et de suppression des Données	**Obligation devant figurer dans le contrat de sous-traitance.** Traiter les Données sur instructions documentées du RT et l'avertir si une instruction est contraire aux règles de protection des Données.
Informer les personnes concernées (ex. politique de confidentialité).	**Obligation devant figurer dans le contrat de sous-traitance.** Veille à ce que son personnel s'engage à respecter la confidentialité des Données.
Permettre aux personnes concernées d'exercer leurs droits et s'assurer de leur respect conformément aux délais prévus par le RGPD.	**Obligation devant figurer dans le contrat de sous-traitance.** Aider, par des mesures organisationnelles et techniques, le RT à donner suite aux demandes d'exercice des droits par les personnes concernées.
Assurer la sécurité des Données	**Obligation devant figurer dans le contrat de sous-traitance.** Assurer un niveau de sécurité des Données adapté aux risques et aider le RT à assurer la sécurité des Données.

Signaler les violations de Données à la CNIL en 72h maximum après en avoir eu connaissance et notifier la CNIL et les personnes concernées, le cas échéant.	**Obligation devant figurer dans le contrat de sous-traitance.** Notifier au RT toute violation de Données et aider ce dernier à remplir ses obligations de notification de la CNIL et des personnes concernées, le cas échéant.
Respect du principe de « Privacy by design and by default » (minimisation des Données, sécurité, etc.).	Prise en compte du principe de « Privacy by design and by default » dans la conception des outils, applications, etc. (ex. Permettre au client de choisir les Données qu'il veut collecter en évitant les champs obligatoires des formulaires, lui permettre de supprimer les Données).
Coopération avec la CNIL dans l'exécution de ses missions.	**Obligation devant figurer dans le contrat de sous-traitance.** Au terme du contrat, sur instruction du RT, supprimer les Données du RT ou détruire les copies existantes (sauf obligation légale de les conserver)
Réaliser des analyses d'impact, le cas échéant.	Aider le RT à réaliser ses analyses d'impact, le cas échéant.
Consultation préalable de la CNIL pour les Traitement nécessitant une analyse d'impact ET présentant un risque élevé pour les personnes concernées persistant après réalisation de l'analyse d'impact.	**Obligation devant figurer dans le contrat de sous-traitance.** Mettre à disposition du RT les informations nécessaires pour démontrer le respect de ses propres obligations et permettre la réalisation d'audits.
Désignation d'un DPO, le cas échant.	Désignation d'un DPO, le cas échant.
Encadrement des Transferts de Données hors UE par un instrument juridique approprié (clauses contractuelles types, etc.).	**Obligation devant figurer dans le contrat de sous-traitance.** Demander l'autorisation du RT en cas de recours à un ST ultérieur, et si Transfert de Données recourir à un instrument de garantie adéquat.
Conclure un contrat de sous-traitance avec chacun de ses ST, conforme à l'article 28 du RGPD.	Conclure un contrat de sous-traitance avec le RT, conforme à l'article 28 du RGPD.

117. **TRANSPOSITION AUX SPÉCIFICITÉS DU SECTEUR : LE CAS DU TRAITEMENT DE VIDÉOPROTECTION.**
L'Enseigne qui conclut un contrat avec le fournisseur d'un dispositif de vidéoprotection s'assure qu'il contient obligatoirement :

- L'objet du traitement (par exemple, des enregistrements de vidéosurveillance des personnes concernées entrant et sortant d'un magasin physique) ;
- La durée du traitement ;
- La nature du traitement (par exemple, enregistrement) et la finalité du traitement (par exemple, la détection d'une entrée illégale) ;

- Le type de données à caractère personnel (par exemple, des images vidéo de personnes concernées entrant et sortant des magasins physiques) ;
- Les catégories de personnes concernées (par exemple, « Clients ») ;
- Les obligations et les droits du Sous-traitant, qui sont celles visées dans le tableau ci-dessus visé à l'article 28.3 du RGPD.

118. **EXIGENCE AUDITABLE (4) : LA VERIFICATION DE LA BONNE REPARTITION DE LA RESPONSABILITE CONJOINTE**. En cas de responsabilité conjointe avérée – c'est-à-dire reflétant la réalité du traitement conjoint - l'Enseigne s'engage à ce que l'accord qui lie les deux responsables conjoints de traitement définisse bien les principes et obligations respectives, listés ci-après, et que ces obligations sont bien réparties entre les deux acteurs afin que chacun soit pleinement informé des obligations qui lui incombe :

- La mise en œuvre des principes généraux de la protection des données ;
- La base juridique du traitement ;
- Les mesures de sécurité ;
- La notification d'une violation de données à caractère personnel à la CNIL et aux personnes concernées ;
- Les analyses d'impact relatives à la protection des données ;
- Le recours à un Sous-traitant ;
- Le Transfert de données vers des pays tiers ;
- L'organisation de contact avec les personnes concernées et les autorités de contrôle ;
- La mise à disposition des grandes lignes de l'accord aux personnes concernées.

L'Enseigne s'engage à documenter les facteurs pertinents et l'analyse menée en interne qui l'a conduit à l'attribution des différentes obligations prévus dans l'accord. Elle doit être attentive aux termes de l'accord afin qu'il précise bien les rôles respectifs en ce qui concerne notamment l'exercice des droits des personnes concernées, et leurs obligations respectives en ce qui concerne les informations visées aux articles 13 et 14 du RGPD. Les responsables conjoints du traitement doivent donc s'organiser et convenir de la manière dont les informations seront communiquées et par qui et de la manière dont les réponses aux demandes de la personne concernée seront fournies et par qui.

3.4. Encadrement des Transferts de Données Personnelles en dehors de l'Union Européenne

3.4.1. Rappel de la règle
3.4.2. Traduction de la règle juridique au commerce de détail

3.4.1. Rappel de la règle

119. **LE PRINCIPE**. Il résulte de la Réglementation Informatique et Libertés, que les Responsables de traitement et les Sous-traitants ne peuvent, en principe transférer[113] , c'est-à-dire communiquer par transmission ou rendre accessible par un autre moyen des Données vers un ou des importateurs situés dans un pays tiers ou une organisation internationale que sous certaines conditions.

120. **LES TROIS CONDITIONS**. Ce principe d'interdiction souffre toutefois de trois exceptions, sous réserve de l'utilisation d'un outil de protection prévu au Chapitre V du RGPD, tels que :

- **Une décision d'adéquation** : Les Transferts sont possibles lorsqu'ils sont réalisés vers un Destinataire établi dans un pays reconnu par la Commission européenne comme offrant un niveau de protection adéquat, conformément à l'article 45 du RGPD.
  A date, ces pays sont : Andorre, Argentine, Canada[114], Iles Féroé, Ile de Man, Ile de Guernesey, Ile de Jersey, Uruguay, Suisse, Nouvelle-Zélande, Israël, Lichtenstein, Islande, Norvège, Japon[115], le Royaume-Uni[116] depuis le 28 juin 2021, la Corée du Sud, les Etats-Unis[117] et très prochainement le Brésil. Il faudra aussi tenir compte d'une nouvelle décision d'adéquation pour l'organisation européenne des brevets.
  L'Enseigne reconnaît que cette liste est susceptible d'évoluer.

[113] Voir définition « transfert » p.12

[114] Uniquement dans le cadre de la loi canadienne sur la protection des renseignements personnels et documents électroniques du 13 avril 2000. Selon la CNIL, « *cette loi s'applique aux organisations du secteur privé qui collectent, utilisent ou communiquent des données personnelles dans le cadre d'activités commerciales, dans la mesure où ces entreprises relèvent du champ d'application de la loi fédérale* » (*Guide Transferts de données à caractère personnel vers des pays non-membres de l'Union Européenne, CNIL, juin 2008*).

[115] Le Japon est limité à la loi sur la protection des informations personnelles (APPI) qui exclut notamment certains traitements liés au secteur public.

[116] Décision d'exécution de la Commission européenne du 28 juin 2021 constatant le niveau de protection adéquat des données personnelles assuré par le Royaume-Uni au titre du RGPD (https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_fr_0.pdf)

[117] Cette adéquation n'étant que partielle, il convient de s'assurer que l'organisme destinataire des données soit bien inscrit sur une liste mise à disposition sur le site du Département du Commerce des Etats-Unis (Décision d'adéquation de la Commission européenne en date du 10 juillet 2023).

- **Des garanties appropriées** : En l'absence de décision d'adéquation (i.e si le pays visé par les Transferts ne figure pas parmi la liste de la Commission européenne)[118], le Transfert de Données n'est possible qu'à la condition que les Responsables de traitement et les Sous-traitants, en tant qu'importateurs ou exportateurs de données mettent en place des garanties appropriées, assurant aux personnes concernées des droits opposables et des voies de recours effectives. Ces garanties appropriées peuvent notamment résulter des instruments suivants qui sont les plus adaptés aux entités visées par le Code [119] :

  - D'un accord conclu avec le Destinataire des Données et contenant des Clauses Contractuelles Types validées par la Commission Européenne (« *CCT* »)[120] ;

  - De règles d'entreprises contraignantes acceptées au sein d'un groupe (« *BCR* » - « *Binding Corporate Rules* »)[121]. Cette dernière hypothèse concerne le cas des Transferts de Données intra-groupe ;

  - D'un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le Sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

- **Une des situations particulières suivantes** : En l'absence de décision d'adéquation ou de garanties appropriées dans les conditions susmentionnées, les Transferts ne sont notamment possibles, selon l'article 49 du RGPD, que si alternativement (i) la personne concernée a donné son consentement explicité au Transfert envisagé, après avoir été informée des risques, (ii) le Transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le Responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée, (iii) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale; (iv) le Transfert est nécessaire pour des motifs importants d'intérêt public, (v) le Transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice, (vi) le Transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, ou (vii) le transfert a lieu au départ d'un registre qui,

[118] Voir : https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[119] Article 46 RGPD
[120] Transfert de données : les clauses contractuelles types (CCT) de la Commission européenne - CNIL
[121] Article 47 RGPD

conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce. [122]

3.4.2. Traduction de la règle juridique au commerce de détail

121. Lorsque l'Enseigne souhaite procéder à un Transfert de données vers un pays ne bénéficiant pas d'une décision d'adéquation, elle suit la démarche ci-après exposée.

122. La CNIL établit une approche en six étapes pour aider les responsables de traitement et les sous-traitants à évaluer les pays tiers et à identifier les mesures complémentaires adaptées par la réalisation d'une Analyse d'Impact des Transferts de Données (« AITD »).

L'Enseigne s'appuie sur les tableaux élaborés par la CNIL pour chaque étape de cette démarche[123].

123. Les six étapes sont les suivantes :

- **Etape 1 : Description des Transferts.** L'Enseigne doit réaliser une cartographie de ses Transferts afin d'identifier :
  - L'exportateur et l'importateur ; et
  - Les caractéristiques du Traitement (i.e type de transfert, fréquences des transferts, catégories de Données transférées, personnes vulnérables parmi les personnes concernées, possibilité d'effectuer des Transferts ultérieurs, volume de Données transférées, etc.).

  Pour ce faire l'Enseigne est invitée à compléter le tableau de la CNIL[124].

- **Etape 2 : Identification de l'outil de transfert adéquat.** En l'absence d'une décision d'adéquation, comme mentionné précédemment, l'Enseigne doit déterminer l'outil de transfert qu'elle envisage d'utiliser conformément à l'article 46 du RGPD (voir *infra*).

  Si l'Enseigne choisit un outil mentionné à l'article 46, la CNIL estime qu'une AITD est nécessaire, impliquant ainsi de passer à l'étape 3 (voir *supra*), qui consiste à évaluer la législation et les pratiques du pays de destination des

[122] En l'absence de ces conditions, les transferts doivent respecter les conditions déterminées à l'article 49 du RGPD et dans les lignes directrices 2/2018 du 25 mai 2018 relatives aux dérogations prévues à l'article 49 du RGPD (https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf)

[123] Guide pratique de la CNIL - Analyse d'impact des transferts des données

[124] Guide pratique - Analyse d'impact des transferts de données - Version finale, pages 12 à 15. La CNIL a partagé un modèle d'AITD qui peut être directement complété.

données. Dans ce cas, l'Enseigne est invitée à compléter le tableau fourni par la CNIL[125].

En revanche, si aucun outil de l'article 46 n'est utilisé et que le Transfert repose sur l'une des exceptions prévues à l'article 49 (voir ci-dessus), la réalisation d'une AITD n'est pas obligatoire. Dans cette situation, l'Enseigne doit toutefois justifier et documenter sa décision de ne pas procéder à cette analyse [126].

- **Etape 3 : Evaluation de la législation et des pratiques du pays de destination de données**. Cette étape permet à l'Enseigne, en qualité d'exportateur de données, de déterminer, en collaboration avec l'importateur, s'il existe des éléments dans la législation ou les pratiques du pays tiers importateur qui pourraient porter atteinte à l'efficacité des garanties de l'outil utilisé, dans le contexte spécifique du transfert, ou empêcher l'exportateur ou l'importateur de remplir leurs obligations.

  L'Enseigne devra donc prendre en compte l'état du droit, le respect des droits de l'homme et des libertés fondamentales, la législation sectorielle, la jurisprudence, les droits effectifs opposables dont bénéficient les personnes concernées, les recours administratifs et judiciaires que peuvent introduire les personnes concernées, l'existence et le fonctionnement effectifs d'une ou plusieurs autorités de contrôle indépendantes, et les engagements internationaux par le pays tiers en question[127].

  Pour ce faire l'Enseigne est invitée à compléter le tableau de la CNIL[128].

- **Etape 4 : Evaluation des mesures existantes et nécessité d'adopter des mesures supplémentaires.** L'Enseigne doit identifier pour chaque Traitement quelles mesures supplémentaires pourraient être efficaces pour le Transfert vers un pays tiers donné (mesures de pseudonymisation, de chiffrement des données ect). Le CEPD donne des exemples de mesures supplémentaires illustrés par des cas d'usage[129].

  Pour ce faire l'Enseigne est invitée à compléter le tableau de la CNIL[130].

- **Etape 5 : Evaluation de l'efficacité des mesures supplémentaires.** Une fois les mesures supplémentaires adéquates identifiées afin de garantir un niveau

[125] Guide pratique - Analyse d'impact des transferts de données - Version finale, page 16. La CNIL a partagé un modèle d'AITD qui peut être directement complété.

[126] Guide pratique de la CNIL, précité, page 16 et modèle d'AITD de la CNIL, précité.

[127] Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, Annexe 3 « Sources d'information possibles aux fins de l'évaluation d'un pays tiers »

[128] Guide pratique de la CNIL, précité, pages 17 à 23 et modèle d'AITD de la CNIL, précité.

[129] Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, Annexe 2 « Exemples de mesures supplémentaires »

[130] Guide pratique de la CNIL, précité, pages 25 à 28 et modèle d'AITD de la CNIL, précité.

de protection des données transférées équivalent à celui de l'Union européenne, l'Enseigne doit établir la liste des actions à entreprendre pour mettre en place ces mesures et respecter les éventuelles étapes procédurales requises.
Pour ce faire, elle est invitée à compléter le tableau fourni par la CNIL[131].

- **Etape 6 : Réévaluation régulière du respect des Transferts de Données Personnelles hors Union européenne.** L'Enseigne doit réévaluer à intervalle régulière (la CNIL donne un exemple de deux ans pour la réévaluation[132]) si l'ensemble des étapes 1 à 5 susmentionnées (i) restent pertinentes pour chaque Transfert de Données et (ii) sont toujours conformes au RGPD.
  Pour ce faire l'Enseigne est invitée à compléter le tableau de la CNIL[133].

124. **EXIGENCE AUDITABLE : DEMARCHE EN CAS DE TRANSFERTS DE DONNEES VERS DES PAYS RECONNUS NON ADEQUATS.** L'Enseigne doit s'assurer de respecter une démarche précise en plusieurs étapes et la documenter afin de valablement transférer des données personnelles vers des pays reconnus non-adéquats :

- La cartographie des transferts ;
- L'identification de l'instrument de transfert adéquat ;
- L'évaluation de l'existence d'un instrument juridique choisi à la lumière des circonstances du transfert ou l'existence de circonstances particulières permettant une dérogation ;
- L'adoption de mesures supplémentaires le cas échéant ;
- La formalisation de la mise en place de ces mesures supplémentaires ; et
- La réévaluation à intervalles réguliers.

L'Enseigne s'assure que chaque transfert de Données s'appuie sur un instrument juridique valable (pays bénéficiant d'une décision d'adéquation ou d'instruments juridiques de transfert tels que les Clauses contractuelles types de la Commission européenne ou les BCR par exemple) ou qu'il existe une circonstance particulière permettant une dérogation au titre de l'article 49 du RGPD.

3.5. Obligation de sécurité

3.5.1. La mise en œuvre de mesures appropriées
3.5.2. Notification en cas de violation de données

[131] Guide pratique de la CNIL, précité, pages 29 à 30 et modèle d'AITD de la CNIL, précité.
[132] Guide pratique de la CNIL, précité, page 30 et modèle d'AITD de la CNIL, précité.
[133] Guide pratique de la CNIL, précité, page 30 et modèle d'AITD de la CNIL, précité.

3.5.1. La mise en œuvre de mesures appropriées

125. **RAPPEL DE LA RÈGLE**. L'Enseigne, en qualité de Responsable de Traitement, est tenue à une obligation de sécurité des Données afin d'éviter que celles-ci ne soient déformées, endommagées, ou que des tiers non autorisés y aient accès[134]. La sécurité des Données doit couvrir tous les aspects du Traitement, tant au niveau organisationnel que technique, à travers l'accès, la Conservation et la communication (Art. 32 RGPD).

126. **TRADUCTION DE LA RÈGLE JURIDIQUE AUX PRATIQUES SECTORIELLES.** L'Enseigne doit mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* »[135]. En pratique, la détermination des mesures adéquates dépend de « *l'état des connaissances* » des risques identifiés, ainsi que des « *coûts de mises en œuvre* »[136]. En d'autres termes, l'Enseigne s'engage à mener :

- Une analyse de risques orientés vers les droits fondamentaux des personnes concernées par l'ensemble des traitements, de façon à pouvoir arbitrer sur les mesures de sécurité à mettre en place en tenant compte de leur coût ;
- Une fois cette analyse réalisée, l'Enseigne définit les mesures propres à y répondre ;
- Ces mesures appropriées sont ensuite consolidées dans une politique de sécurité des systèmes d'information (aussi appelée la « PSSI »), que l'Enseigne s'engage à formaliser par des mesures adaptées aux risques identifiés.
- Cette PSSI est appliquée grâce à l'élaboration d'une gouvernance de sécurité que l'Enseigne s'engage à mettre en place.

Par ailleurs, il est recommandé pour l'Enseigne de mettre en place un socle de sécurité reprenant les bonnes pratiques issues d'années de capitalisation d'hygiène et de sécurité informatique (ex. : règlementations, normes, guides). Ce socle[137], auquel contribuent les mesures listées ci-après, vise à répondre aux risques les plus courants.

---

[134] Article 4. 6° de la LIL modifiée

[135] Article 32.1 RGPD : « (…) *y compris entre autres, selon les besoins :*
- la pseudonymisation et le chiffrement des Données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

[136] Article 31.2 RGPD

[137] Voir le Guide de la sécurité des données personnelles de la CNIL : https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles

- **Mesures préventives -Prérequis en matière de cadre et gouvernance et exigences auditables**.

127. En adhérant au présent Code de conduite, l'Enseigne s'engage à mettre en place des mesures organisationnelles préventives de sécurité, adaptées à son contexte, qui devront aborder les points suivants :

- **La mise en place d'une politique de la sécurité**

Politique et/ou charte de sécurité relative aux données personnelles. Cette politique ou charte, induite par la nature des menaces identifiées, implique notamment de dégager une classification des données (stratégiques, critiques, non sensibles, etc.), qui seront ensuite soumises à des restrictions d'accès et/ou d'usage adaptées[138].

Revues et évolution de la politique de sécurité relative aux données personnelles. L'Enseigne procède à des examens réguliers de sécurité, de l'adéquation du programme de sécurité défini, et, par conséquent, de la politique de sécurité, puis elle détermine si des mesures de sécurité supplémentaires doivent être adoptées en cas de survenance d'un nouveau risque de sécurité. Dans ce cas, elle communique l'information au personnel.

- **La mise en place d'une gouvernance de la sécurité**

Personnes responsables de la sécurité des données personnelles et rôles/responsabilités des équipes afférentes. La responsabilité de la mise œuvre de cette politique (PSSI) est confiée à une entité interne dédiée, impliquant :

- La désignation/nomination d'un Responsable de la sécurité des systèmes d'information (RSSI) ou équivalent ;
- L'octroi de moyens humains et financiers adaptés ;
- L'implication du RSSI dans toute initiative stratégique ou tout nouveau projet afin d'être en mesure d'identifier les éventuels risques pour y apporter une réponse systématique adaptée ;
- La définition claire et précise du rôle et des responsabilités du RSSI, comprenant un fort partenariat avec la direction de l'entreprise.

[138] La politique de gestion interne des incidents de sécurité doit, **par exemple,** permettre de :

- détecter immédiatement une violation et à l'endiguer rapidement ;
- traiter ces incidents, y compris sur la personne responsable de cette gestion des incidents ;
- effectuer des enquêtes rapides lorsqu'une Enseigne a connaissance d'une violation présumée afin de déterminer si une violation a eu lieu et quelles données personnelles sont affectées ;
- analyser les risques engendrés par l'incident ;
- atténuer l'impact potentiel et à remédier aux vulnérabilités révélées par cet incident ;
- déterminer s'il convient de notifier l'autorité de contrôle, voire les personnes concernées ;
- tenir un registre des violations de données

L'application de la PSSI aux interlocuteurs internes et externes

Afin de se protéger des menaces, l'Enseigne met en place des mesures tant à l'égard de ses collaborateurs, qu'à l'égard de ses prestataires et partenaires, afin qu'ils puissent informer la direction de l'Enseigne de tout incident ou menace relative à la sécurité.

✓ <u>À l'égard de ses collaborateurs</u>

- **Campagnes de formation et/ou de sensibilisation des collaborateurs en matière de risque et de protection de l'information – en particulier des personnes ayant un accès important aux données.** Actions d'information, de sensibilisation et de formation permettant d'expliquer les risques et menaces pesant sur les données, identifier les situations et comportements à risque, ainsi que leur impact potentiel, établissement d'une documentation accessible et qui détaille les règles de sécurité applicables aux données de l'organisation ;

- **Implication des collaborateurs.** Comportement à adopter pour garantir la sécurité, capacité de signalement et d'alerte vers les équipes du RSSI lorsque les atteintes portent sur les systèmes qu'ils opèrent ;

- **Outillage des collaborateurs.** Mise en place d'outils permettant d'automatiser les mécanismes de protection ; adaptés aux profils des risques identifiés et devant régulièrement être revus, se traduisant notamment par la mise en place de (i) contrôle d'accès[139], (ii) le filtrage des flux[140], (iii) le chiffrement[141], et (iv) la détection et la réaction[142].

- **Responsabilisation des collaborateurs.** Opposabilité, à travers un document qui prend généralement la forme d'une charte informatique, permettant de s'assurer que le personnel de l'Enseigne a bien lu et compris la politique de sécurité de l'information et les procédures à mettre en œuvre. Pour avoir valeur contraignante, celle-ci doit : - soit, être intégrée au règlement intérieur de l'entité dont elle constituera une annexe[143] ; - soit, être intégrée au contrat de travail (directement dans la version native, ou ultérieurement par voie d'avenant).

- **Evaluation des collaborateurs.** Organisation de tests face à un scénario de crise.

---

[139] L'objectif est d'autoriser ou de refuser un accès par un utilisateur préalablement identifié et authentifié sur une ressource informatique. L'authentification consiste à s'assurer que l'utilisateur est bien celui qu'il prétend être. Le moyen le plus fréquemment utilisé est le mot de passe.

[140] Il s'agit d'autoriser ou de refuser un flux de données entre deux ressources informatiques, par un dispositif de « firewall » par exemple.

[141] L'objectif est de protéger la confidentialité et l'intégrité des données par une clef de chiffrement.

[142] Des moyens techniques permettant de détecter les attaques, telles que des programmes malveillants, de type virus, ou intrusions par des pirates, sont mis en œuvre.

[143] Sous respect de soumettre ce document au préalable, pour information et consultation, aux organes compétents dans le respect des dispositions du Code du travail.

✓ <u>À l'égard de prestataires et Sous-traitants</u>

- **Application de la PSSI aux prestataires et adoption d'une politique contractuelle stricte.** Sélection rigoureuse des prestataires avant de leur confier quelconque mission, obligation stricte de s'engager contractuellement à respecter des niveaux de sécurité exigées par la politique de l'entreprise, afin d'en garantir notamment la confidentialité.

- **L'analyse des contrats impliquant la gestion de données à caractère personnel de personnes physiques et les contrats fournisseurs par la DSI de l'Enseigne (plan d'assurance sécurité)**

Les contrats doivent comprendre notamment les clauses suivantes : confidentialité, sécurité (dont les modalités d'authentification), audit, restitution/Destruction des données, notification en cas de violation de données, et responsabilité ; afin que les DSI soient en mesure (i) de préciser et/ou modifier le cas échéant les mesures de sécurité imposées afin que ces dernières correspondent à la réalité de ce que l'Enseigne pratique et de ne pas voir sa responsabilité engagée en cas de violation de données ; (ii) de valider les mesures de sécurité proposées par les fournisseurs.

- **La réalisation d'évaluation ou de tests documentés pour apprécier le niveau de sécurité dans l'Enseigne et chez ses Sous-traitants**

L'Enseigne réalise des audits réguliers de sécurité afin de s'assurer que les Sous-traitants auxquels elle a recours respectent bien les instructions induites des mesures prévues dans sa PSSI.
A contrario, le Sous-traitant doit respecter avec rigueur les instructions de l'Enseigne Responsable de traitement pour ne pas voir sa responsabilité engagée.

➢ **Moyens organisationnels de protection et de mise en application de la politique de sécurité**.

128. **En prévention d'incident**, l'Enseigne s'engage à :

- Appliquer les politiques de sécurité dans les processus de développement, d'acquisition (chaîne d'approvisionnement) et de maintien en condition opérationnelle des systèmes hébergeant des données personnelles ;
- Disposer de normes et procédures permettant d'analyser les risques, notamment :
  - D'identifier l'événement redouté, sa nature et son niveau de gravité[144] ;
  - D'identifier et de caractériser la source du risque[145] ;

[144] Impact : humain, organisationnel, financier, juridique, image / gravité : critique, grave, significatif, mineur
[145] Source non intentionnelle : erreur humaine, oubli / Source intentionnelle : fraude, détournement d'usage, falsification, sabotage, agitation etc.

- De cartographier l'écosystème (parties prenantes telles que les services internes, les clients, les partenaires) ;
- De qualifier le niveau d'exposition[146] ;
- De caractériser le niveau de menaces à partir du niveau d'exposition, des sources de risques et de l'écosystème ;
- De déterminer le niveau de vraisemblance de l'occurrence de l'événement redouté et de la difficulté technique du scénario opérationnel[147] ;
- De déterminer les mesures de sécurité adaptées aux niveaux de menaces

- Procéder à des analyses de risques de manière périodique et pour les cas où un événement représentant un risque pour les données survient (exemples : mise en place de nouveaux traitements, implémentation de nouveaux projets SI).
- Disposer d'une procédure permettant d'identifier les incidents de sécurité sur les données et de mettre en place un plan de remédiation pour endiguer rapidement la violation.

129. **EXIGENCE AUDITABLE : LA MISE EN PLACE DE MESURES DE SECURITE**. De façon pratique, l'Enseigne prend les engagements de mettre en place les mesures suivantes :

- **Sensibiliser ses salariés accédants aux données des Prospects / Clients** => Elle rédige une charte informatique comprenant les mentions suivantes : un rappel des règles sur la protection des données, les modalités d'intervention des équipes chargées de la gestion des ressources informatiques, les moyens d'authentification, les règles de sécurité auxquelles les salariés doivent se conformer (signaler au service informatique interne toute violation, et de manière générale tout dysfonctionnement, ne jamais confier son identifiant / mot de passe à un tiers, verrouiller son ordinateur en quittant son poste de travail), les modalités d'utilisation des moyens informatiques mis à disposition (poste de travail, caisses, Internet, messagerie électronique, téléphonie), les conditions d'administration du système d'information (systèmes de filtrage et de traçabilité), les responsabilités.

Par exemple, chaque salarié des magasins de vente physique est sensibilisé sur l'impératif de ne jamais laisser un poste de caisse sans surveillance. Également, dans l'hypothèse où l'Enseigne propose un formulaire papier en magasins de vente physique permettant aux Personnes concernées d'exercer leurs droits ou encore pour souscrire à un programme de fidélité, elle indique en en-tête ou pied de page du document de la mention selon laquelle le document comprend des données à caractère personnel, afin de sensibiliser l'attention portée par les Clients et les salariés.

- **Authentifier les salariés accédants aux données et les Utilisateurs** => Elle instaure l'élaboration d'un identifiant unique distinct pour chaque salarié et Utilisateur en cas de création de compte en ligne et applique des mesures pour authentifier ces derniers. Quand des mots de passe sont utilisés, l'Enseigne applique une politique de

[146] Système très accessible, moyennement accessible ou peu accessible

[147] Vraisemblance quasi-certaine, très élevée, significative, faible, très faible / Difficulté négligeable, faible, modéré, élevé, très élevé

mots de passe conforme aux recommandations de la CNIL[148], en particulier, ces mots de passe doivent :

- Être d'une complexité suffisante, c'est-à-dire, par exemple, comprendre au moins 8 caractères comportant les 4 types de caractères (majuscules, minuscules, chiffres, caractères spéciaux) si l'authentification prévoit une restriction d'accès au compte comme une temporisation d'accès au compte après plusieurs échecs, un mécanisme déterminant un nombre maximal de tentatives autorisées dans un délai donné (par exemple, 10 essais par heure), un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (par exemple : mise en œuvre de « captcha ») ou un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10, assorti d'un mécanisme de déblocage proportionnel aux risques que les personnes fassent l'objet d'une usurpation d'identité[149] ;
- Les mots de passe des utilisateurs doivent être stockés sous la forme d'une empreinte cryptographique (hash) via une fonction spécifiquement adaptée ;
- Respecter tout autre règle d'application générale plus exigeante que l'autorité de contrôle pourrait être amenée à adopter au cours de l'application du présent Code.

Par exemple, chaque salarié, nonobstant le poste qu'il occupe, dispose d'un identifiant unique assorti d'un mot de passe conforme. Également, pour toute création de compte en ligne par un Utilisateur, celle-ci est conditionnée à la définition d'un mot de passe robuste conforme.

- **Gérer les habilitations** => Elle définit des profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité, supprime les permissions d'accès des salariés 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, et réalise 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 salarié).

- **Tracer les accès** => Elle enregistre les opérations réalisées par des salariés et Utilisateurs (disposant d'un compte en ligne sur son site), les anomalies et les évènements liés à la sécurité pour une période de six mois minimums et n'excédant pas un an, le système de journalisation devant comprendre l'identifiant, la date et l'heure de la connexion et déconnexion des Utilisateurs. Par ailleurs, dans la mesure du possible, ces traces ne doivent pas conserver d'autres données personnelles et il

[148] Voir la recommandation sur les mots de passes de la CNIL : https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation-2022-100-du-21-juillet-2022_recommandation-aux-mots-de-passe.pdf.

[149] Conformément à la Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017.

est nécessaire de vérifier de ces traces (périodiquement et/ou de manière automatisée).

Par exemple, l'Enseigne trace les accès aux comptes en ligne des Utilisateurs, ainsi que ceux des salariés habilités à la gestion de ces comptes, dans la limite de six mois.

- **Sécuriser les postes de travail** => L'enseigne prévoit :
    - Un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant une durée déterminée ;
    - L'installation d'un « pare-feu » (« firewall ») logiciel,
    - La mise à jour régulière d'antivirus sur les postes ;
    - La configuration des logiciels utilisés pour permettre leur mise à jour de sécurité automatique utilisés lorsque cela est possible ;
    - Le stockage des données sur un espace régulièrement sauvegardé accessible sur le réseau de l'Enseigne et non sur les postes de travail ;
    - Une limitation de connexion de supports mobiles à ce qui est strictement indispensable.

Par exemple, l'Enseigne sécurise les postes de travail faisant office de caisses (« postes nomades ») dans les magasins de vente physiques. De la même manière, elle instaure un dispositif de verrouillage automatique sur lesdites caisses en cas de non-interaction pendant une durée supérieure à ce que l'Enseigne juge raisonnable (inactivité de 1 à 5 minutes), de la même façon qu'elle instaure un dispositif de déconnexion automatique des comptes en ligne des personnes concernées à défaut d'interaction d'une durée supérieure à ce qui est jugé raisonnable par l'Enseigne (inactivité de 1 à 5 min).

- **Sécuriser l'informatique mobile** => L'Enseigne met en œuvre des mécanismes de sauvegarde ou de synchronisation pour se prémunir contre la disparition de données stockées et prévoit des moyens de chiffrement des postes et supports de stockage mobiles (ordinateurs portables, clés USB, disques durs externes, etc.). Concernant les smartphones, l'Enseigne veille à activer le verrouillage automatique du terminal et exige un code secret pour le déverrouiller en plus du code PIN de la carte SIM.

- **Protéger le réseau informatique interne** => L'Enseigne limite les accès internet aux services strictement nécessaires. Lorsqu'elle propose un accès WIFI en boutique, elle le sépare du réseau interne, et utilise dans les deux cas un chiffrement conforme à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe). Elle impose un VPN pour tout accès à distance et s'assure qu'aucune interface d'administration n'est accessible directement depuis Internet.

Par exemple, l'Enseigne qui propose un accès WIFI aux Clients dans ses magasins physiques veille à dissocier cet accès (en créant par exemple un espace « guest » / « invité »), qu'elle conditionne à une authentification fortement sécurisée, à celui de ses salariés de ces mêmes magasins.

- **Sécuriser les serveurs** => L'Enseigne limite l'accès aux outils et interfaces d'administration aux seules personnes habilitées, et installe sans délai les mises à jour

critiques. Elle effectue des sauvegardes régulières qu'elle contrôle et met en œuvre le protocole TLS dans une version 1.2. a minima[150].

- **Sécuriser les sites web** => L'enseigne met en œuvre (a minima) la version 1.2. du protocole TLS sur tous ses sites web et rend son utilisation obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des Données personnelles. Elle limite, également, l'accès aux outils et interfaces d'administration aux seules personnes habilitées.

Par exemple, l'Enseigne utilise le protocole TLS (HTTPS) pour assurer l'authentification des serveurs et la confidentialité des communications et privilégie le recours à un prestataire de service de certification électronique référencé comme conforme au RGS[151] dans sa version 1.0 pour un usage d'authentification de serveur. Pour les sites disposant d'un agent conversationnel (chatbot), elle demande aux Utilisateurs de faire attention à ce qu'ils écrivent, d'éviter de donner des vraies données dans les formulaires d'information sur les Utilisateurs, de ne pas faire confiance aux pièces jointes (ne pas lancer des fichiers provenant d'inconnus), de ne pas suivre tous les liens hypertextes.

- **Sauvegarder et prévoir la continuité d'activité** => L'enseigne effectue des sauvegardes fréquentes des données papiers ou électroniques et met en place des sauvegardes incrémentales quotidiennes et complètes à intervalles réguliers. Elle stocke ses sauvegardes sur un site extérieur (dans des coffres ignifugés ou étanches). Elle adopte un même niveau de sécurité pour les données sauvegardées que celles mises en place pour les données stockées sur les serveurs d'exploitation. Par ailleurs, elle rédige un plan de reprise et de continuité d'activité et elle teste régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.

- **Archiver de manière sécurisée** => L'Enseigne définit un processus de gestion des archives et met en œuvre des modalités d'accès aux données archivées. S'agissant de la Destruction des archives, l'Enseigne s'attache à mettre en place un mode opératoire garantissant que l'intégralité des archives concernées a bien été détruite.

- **Encadrer la maintenance et la Destruction des données** => L'Enseigne documente toute intervention de maintenance effectuée par un tiers, laquelle est systématiquement encadrée par un responsable, et prévoit une clause de sécurité dans les contrats de maintenance qu'elle signe avec des prestataires. Elle met en œuvre une politique de suppression sécurisée des données.

[150]Voir les Recommandations de sécurité relatives à TLS de l'ANSSI : https://messervices.cyber.gouv.fr/guides/recommandations-de-securite-relatives-tls

[151] Voir le Référentiel général de sécurité proposant un cadre réglementaire de l'ANSSI : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

- **Gérer la sous-traitance** => L'Enseigne réalise une évaluation ou des tests documentés (rapports d'audits, templates de questionnaires, fiche d'évaluation etc.) pour apprécier le niveau de sécurité chez ses sous-traitants.

- **Sécuriser les échanges avec d'autres organismes** => L'Enseigne chiffre les données avant tout enregistrement sur un support physique qu'elle transmet à un tiers. Lors d'un envoi via un réseau, elle chiffre les pièces sensibles à transmettre en cas d'utilisation de messagerie électronique, elle assure la confidentialité des mots de passe et clés de chiffrement en les transmettant via un canal distinct. Enfin, elle utilise un protocole garantissant la confidentialité et l'authentification du serveur Destinataire pour les Transferts de fichiers.

- **Protéger les locaux** => L'enseigne veille à installer des alarmes anti-intrusion périodiquement contrôlées, des détecteurs de fumée ainsi que des moyens de lutte contre les incendies qui sont annuellement inspectées, et établir des règles et moyens de contrôle d'accès.

Par exemple, l'Enseigne met en place des moyens humains (vigils) et techniques pour contrôler les accès et sécuriser les lieux.

- **Encadrer les développements informatiques** => Pour tout développement de ses sites internet ou applications mobiles par exemple, à destination des personnes concernées, l'Enseigne mène une analyse sur les paramètres relatifs à la vie privée, évite le recours à des zones de texte libre ou de commentaires et effectue des développements informatiques et les tests dans un environnement informatique distinct de celui de production et sur des données fictives ou anonymisées.

Par exemple, si l'Enseigne dispose d'une application mobile dédiée, elle peut inviter l'Utilisateur à changer les paramètres par défaut. Elle permet à l'Utilisateur de s'opposer à la Collecte de données particulières (coordonnées bancaires notamment). Elle prévient l'Utilisateur (icône, voyant lumineux) quand l'application fonctionne en arrière-plan, quand l'appareil "écoute" avec le micro, quand la localisation est collectée, etc. et lui permet de s'y opposer. Enfin, elle propose un dispositif de contrôle parental, afin d'exclure les enfants de moins de 13 ans de tout traitement de profilage automatisé ; et elle arrête effectivement toute Collecte de données si l'Utilisateur retire son consentement.

- **Utiliser des fonctions cryptographiques** => L'Enseigne :
  - utilise un algorithme reconnu et sûr, ainsi que des tailles de clé de chiffrement suffisantes ;
  - met en place des accès restrictifs et des mots de passe pour protéger les clés de chiffrement ;
  - enfin, elle rédige une procédure indiquant la manière dont les clés et les certificats sont gérés.

Par exemple, l'Enseigne emploie des outils (dispositifs de protection des clés privées, module de chiffrement et module de déchiffrement) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information (ANSSI) au niveau correspondant à la robustesse attendue. S'agissant des matériels utilisés,

l'Enseigne utilise des équipements chiffrables tels que des disques durs avec une technologie SED, ou des logiciels tels que dm-crypt sous Linux, FileVault sous MacOS, VeraCrypt sous Windows[152]*. Enfin, l'Enseigne chiffre les données des fichiers stockés ou les pièces à joindre à des courriers électroniques (logiciels tels que ZoneCentral, ceux utilisant la librairie Security BOX Crypto 6.0, ou encore AxCrypt ou Gnu Privacy Guard (GPG). A défaut, elle utilise au moins un outil de compression qui permet de chiffrer avec mot de passe, tel que 7-Zip qui permet le chiffrement AES, ou bien recourir à une solution matérielle telle qu'une carte Bull Trustway PCI cryptographic card, etc.)*[153].

- **Mettre en œuvre une politique de sécurité et de gouvernance** => L'Enseigne :
  - s'assure de disposer d'une politique ou d'une charte de sécurité relative aux données personnelles ;
  - de mettre en place une procédure de révision de ce document.
  - désigne une ou des personnes responsables de la sécurité des données personnelles, avec des rôles clairement définis et des moyens adéquats pour le bon fonctionnement de leurs missions.
  - procède à des analyses de risques de manière périodique.
  - dispose d'une procédure permettant d'identifier les incidents de sécurité sur les données et de mettre en place un plan de remédiation pour endiguer rapidement la violation.

ILLUSTRATIONS PRATIQUES

Constituent, par exemple, des manquements à l'obligation de sécurité le fait :

- *D'omettre de prévoir des restrictions d'accès aux images captées par des dispositifs de vidéoprotection et surveillance*[154] *;*
- *De conserver des numéros de cartes bancaires stockés « en clair dans les champs commentaires » d'une base de données*[155] *;*
- *De ne pas prendre les précautions propres à prévenir tout risque d'erreur en particulier en raison d'une homonymie*[156].

[152] PIA, les bases de connaissances (cnil.fr)

[153] PIA, les bases de connaissances (cnil.fr)

[154] CNIL, délibération n° 2014-307, 17 juill. 2014 : dans cette affaire, la CNIL a prononcé une sanction pécuniaire de 5 000 € à l'encontre d'un responsable de traitement, notamment pour avoir mis en place des dispositifs de vidéoprotection et vidéosurveillance, dont les images « restaient accessibles à la totalité du personnel de chaque magasin ».

[155] CNIL, délib. n° 2016-265, 20 sept. 2016.

[156] CA Paris, 15 févr. 1994, n° 93/03512. V. également Cass. crim., 19 déc. 1995, n° 94-81.431 : « une personne ayant le même patronyme et la même date de naissance, mais demeurant dans le Val-de-Marne, s'est vue d'une part refuser un crédit à la consommation par un grand magasin et, d'autre part, relancée par un organisme de crédit ayant à l'origine donné le signalement du mauvais payeur ; (…) c'est en raison d'une absence de précautions dans la collecte, l'enregistrement, et la diffusion des éléments de l'état civil des personnes en cause – une absence systématique d'enregistrement du

3.4.3. Notification en cas de violation de données

130. **RAPPEL DE LA RÈGLE**. L'article 4.12. du RGPD définit la « violation de données » comme une « *violation de la 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* ».

131. L'Enseigne met en place des mesures pour prévenir et limiter les risques de violations de données à caractère personnel et réagir de manière appropriée en cas d'incident[157], c'est-à-dire en cas de violation de données à caractère personnel[158].

132. En cas d'incident de sécurité ayant un impact sur les données personnelles (vol de données, accès non autorisé, perte / panne d'un équipement contenant des données, les Destruction ou divulgation accidentelle de ces dernières, etc.) l'Enseigne met en place des procédures pour analyser l'impact de la violation sur les personnes concernées.

133. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL.** En cas de violation, l'Enseigne documente la violation au fur et à mesure qu'elle suit les étapes suivantes :

- Elle détermine le type de violation survenue en la catégorisant parmi les trois suivantes : (i) violation de confidentialité, en cas de divulgation ou un accès non autorisé ou accidentel à des DCP ; (ii) violation de l'intégrité, en cas d'altération non autorisée ou accidentelle aux DCP ; (iii) violation de la disponibilité, en cas de perte accidentelle ou non autorisée de l'accès à des DCP ou Destruction[159] ;
- Elle effectue une analyse du risque : à cet effet, elle doit s'interroger sur les effets et les conséquences de cette violation sur les personnes concernées, notamment si leurs données sont divulguées – et donc compromises – ou rendues indisponibles pour une durée plus ou moins longue, ou encore que cette violation soit susceptible de leur occasionner un préjudice. Lors de l'évaluation du niveau des risques, doivent notamment être pris en compte la nature, la sensibilité, le volume des données à caractère personnel concernées par la violation, ainsi que le contexte de l'attaque ;
- L'Enseigne doit notifier la violation à la CNIL dans un délai de soixante-douze (72) heures au plus tard après avoir pris connaissance de la violation en cas de risque pour

lieu de naissance rendant possible les homonymies – que la déformation reprochée avait dû se produire ».

[157] Articles 33 et 34 du RGPD

[158] L'article 4.12) du RGPD définit une violation de données à caractère personnel comme « *une violation de la 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.* ».

[159] CEPD, *Guidelines 01/2021 on Examples regarding personal data breach notification, adopted on 14 December 2021*

les Personnes concernées et la notifier aux Personnes concernées lorsque ce risque est élevé (ex. nombre important de personnes concernées, données sensibles, etc.).

134. **Le contenu précis de la notification**. La notification doit comprendre : (a) une description de la nature de la violation ; (b) si possible, les catégories et le nombre approximatif de personnes concernées par la violation ; (c) les catégories et le nombre approximatif ou estimé de données personnelles concernées par la violation ; (d) les noms et coordonnées du DPO, ou tout autre point de contact pertinent ; (e) les conséquences probables de la violation ; et (f) les mesures prises ou proposées pour remédier ou atténuer les conséquences négatives de la violation[160]. La CNIL propose un téléservice dédié aux Responsables de traitement permettant de lui notifier une violation, accessible à l'adresse suivante : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

135. **L'information des personnes concernées**. Lorsqu'un risque élevé est avéré pour les personnes concernées, l'Enseigne leur notifie la violation dans les meilleurs délais. L'information des personnes concernées est claire et facilement compréhensible. Elle doit décrire la nature de la violation, les noms et coordonnées du DPO (ou autre point de contact), les conséquences probables de cette violation, et les mesures prises/proposées pour y remédier[161].

136. **L'exception à l'obligation d'information**. Par exception, l'Enseigne est dispensée de l'obligation d'information individuelle des personnes concernées, si elle démontre :

- Qu'elle a déjà mis en œuvre des mesures techniques et organisationnelles appropriées rendant les données incompréhensibles à toute personne non autorisée, en chiffrant les données avec un algorithme réputé fort et que la clé de chiffrement n'a pas été compromise lors de l'incident. ;
- Que des mesures ultérieures ont été prises garantissant la disparition du risque élevé pour les droits et libertés des Personnes ;
- Qu'une information individuelle des personnes concernées exigerait des « *efforts disproportionnés* », auquel cas l'Enseigne procède à une communication publique ou une mesure similaire permettant d'informer lesdites Personnes[162].

137. Enfin, l'Enseigne consigne dans une documentation les détails concernant toutes les violations constatées, comprenant les faits, leurs effets et les mesures prises pour y remédier[163].

138. **EXIGENCE AUDITABLE : MISE EN PLACE D'UNE GESTION INTERNE EN CAS DE VIOLATION DES DONNEES**. En cas d'incident représentant des risques pour les personnes concernées, l'Enseigne met en œuvre :

[160] Article 33.3 du RGPD
[161] Article 34.2 du RGPD
[162] Article 34.3 du RGPD
[163] Article 33.5 du RGPD

- Des mécanismes permettant d'identifier rapidement une violation de données et d'évaluer son niveau de gravité (ex. système d'alerte, équipe dédiée),
- Des procédures pour permettre à l'entreprise de prévenir la CNIL dans les meilleurs délais, et au maximum dans un délai de soixante-douze (72) heures suivant la découverte de l'incident,
- Des procédures qui permettent à l'entreprise de prévenir les personnes concernées, de manière individuelle ou au moyen d'une communication publique dans les hypothèses où une communication individualisée représente des efforts disproportionnés.

L'Enseigne s'engage à tenir une documentation (ou registre) détaillée des violations constatées, dans laquelle sont consignés tous les incidents de sécurité ayant un impact avéré ou potentiel sur les données personnelles, leurs effets et les mesures prises pour y remédier.

3.6. Registre des traitements

139. **Rappel pédagogique**. Conformément à l'article 30.1. du RGPD, l'Enseigne Responsable de Traitement dresse un registre des activités de traitement – qu'elle remet à l'Organisme de contrôle lors de sa demande d'adhésion[164]. Un modèle de registre (à personnaliser au cas par cas), agrégeant les référentiels du Code, est proposé en **Annexe A**.

3.7. Délégué à la protection des données personnelles (DPO)

3.7.1. Les cas de désignation obligatoire d'un DPO
3.7.2. Les modalités de désignation
3.7.3. Les missions du DPO

3.7.1. Les cas de désignation obligatoire d'un DPO

140. **RAPPEL DE LA RÈGLE**. Conformément à l'article 37 du RGPD, le Responsable de traitement désigne notamment un délégué à la protection des données lorsque : *« b) les activités de base […] consistent en des opérations de traitement qui, du fait de leur nature, de leur portée*

[164] Article 30.1. RGPD (RT) « *a) 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 ;*
b) les finalités du traitement ;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
d) les catégories de Destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les Destinataires dans des pays tiers ou des organisations internationales ;
e) 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 ;
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1. »

et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; […] ».

141. **TRADUCTION DE LA RÈGLE JURIDIQUE AU SECTEUR CONCERNÉ**. Dans le secteur de la vente et de la distribution au détail de produits d'équipement de la personne, l'Enseigne Responsable de Traitement doit désigner un délégué à la protection des données (ci-après dénommé "**DPO**")[165] dès lors que ses activités de base[166] consistent en des opérations de traitement exigeant un suivi régulier et systématique à grande échelle[167] des personnes concernées, par exemple de la publicité ciblée :

- Le suivi régulier – c'est-à-dire récurrent et périodique[168] – et systématique – c'est à dire planifié et organisé – des personnes renvoie au **profilage des Clients**. Par exemple, la mise en place d'un programme de fidélité, la publicité comportementale, l'établissement de profils aux fins d'attribution de crédits[169] ;
- Pour apprécier la notion de **grande échelle**, les facteurs à prendre en compte sont, notamment (i) le nombre de personnes concernées, (ii) le volume de données et/ou la variété des différents types de données traitées, (iii) la durée du traitement, (iv) l'étendue géographique du traitement[170]. Est considéré comme étant à grande échelle le traitement de données de géolocalisation en temps réel des Clients d'une chaine internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans la fourniture de ces services[171]. A l'inverse, ne sera pas considéré à grande échelle le traitement de données clients, réalisé par un commerçant indépendant isolé, pour un point de vente unique.

142. **L'exemption de nomination d'un DPO**. Pour les Enseignes non visées par l'obligation de désigner un DPO, elles ont néanmoins la faculté d'en choisir un volontairement. Cette pratique, encouragée, engage alors l'Enseigne à respecter l'ensemble des exigences du présent titre du Code de conduite.

---

[165] Article 37 § 1 RGPD.

[166] Considérant 97 RGPD – Les opérations de traitement de données nécessaires au fonctionnement de l'activité principale de l'organisme (par exemple le traitement des données des clients d'un magasin).

[167] Considérant 91 RGPD – Le traitement à grande échelle désigne une opération visant « *à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, et qui donc peut affecter un nombre important de personnes concernées* ».

[168] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p. 10-11. Le terme « régulier » pouvant revêtir plusieurs significations : « (i) *continu ou se produisant à intervalles réguliers au cours d'une période donnée* ; (ii) *récurrent ou se répétant à des moments fixes* ; (iii) *ayant lieu de manière constante ou périodique* ». Le terme « systématique » pouvant revêtir plusieurs significations : « (i) *se produisant conformément à un système* ; (ii) *préétabli, organisé ou méthodique* ; (iii) *ayant lieu dans le cadre d'un programme général de collecte de données* ; (iv) *effectué dans le cadre d'une stratégie* ».

[169] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p. 11.

[170] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.9.

[171] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.9 et 10.

143. **EXIGENCE AUDITABLE : ETABLIR LA DESIGNATION D'UN DPO**. L'Enseigne s'engage à désigner un Délégué à la Protection des Données et être en mesure de produire la confirmation de cette désignation. Dans le cas où elle considère qu'elle n'est pas soumise à cette obligation de désignation, elle s'engage à produire une analyse écrite et à être en mesure d'en communiquer une copie pour justifier du bienfondé de son choix.

3.7.2. Les modalités de désignation

144. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL.** L'Enseigne met en œuvre et respecte les règles afférentes à la désignation de son DPO, et garantit son indépendance, selon les modalités ci-après exposées :

(i) Les possibilités de désignation

145. L'Enseigne peut :

- *Externaliser la fonction* : outre un membre de son personnel, l'Enseigne peut confier cette mission à un prestataire sur la base d'un contrat de service. Le DPO pourra alors être une personne morale[172], par exemple un organisme extérieur à l'Enseigne tel qu'un cabinet d'avocats ou de conseil, ou encore un prestataire Sous-traitant sous réserve que ses fonctions soient bien séparées de celles effectuées sur instructions du Responsable de traitement[173] ;

- *Mutualiser la fonction au sein d'un groupe* : un groupe d'entreprises peut désigner un seul DPO. C'est par exemple le cas pour un groupe de sociétés ou un réseau de distribution, pour les traitements de données réalisés par les membres du groupe. Dans ce cas, chaque entité revêtant la qualité de « responsable de traitement » procède à la désignation du DPO mutualisé[174] ; le DPO mutualisé doit être « facilement joignable » dans tous les lieux d'établissement des entreprises concernées et fait office de point de contact pour faciliter l'accès de l'autorité de contrôle aux documents et informations nécessaires à l'exécution de sa mission. Il est également point de contact au sein de l'organisme (articles 38 et 39 du RGPD) ainsi qu'à l'égard des personnes concernées.

(ii) Les règles de désignation et le statut du DPO

146. **Une compétence accrue**. En plus de qualités personnelles d'intégrité et d'éthique, le DPO désigné dans chaque Enseigne est professionnellement compétent dans le domaine de la protection juridique des données à caractère personnel[175], et le secteur[176] de la vente

[172] Article 37 § 6 RGPD.
[173] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.18.
[174] A titre d'exemple, cinq entités devront procéder chacune à une désignation, soit cinq désignations au total pour les cinq entités.
[175] Article 37.5 RGPD.
[176] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.11.

au détail d'équipements de la personne, y compris les processus métiers mis en œuvre. A ce titre, il doit disposer d'un certain niveau de connaissances, c'est-à-dire :

- une expertise juridique et technique en matière de protection des données ;
- une connaissance du secteur d'activité, de la réglementation sectorielle et de l'organisation de la structure pour laquelle il est désigné ;
- une compréhension des opérations de traitement, des systèmes d'information et des besoins de l'organisme en matière de protection et de sécurité des données ;

147. **Un référent accessible**. Lors de sa désignation, l'Enseigne fait son affaire de :

- La communication de l'identité et des coordonnées du DPO à l'autorité de contrôle compétente – la CNIL ;
- L'accessibilité au public de ses coordonnées – en les renseignant sur la politique de confidentialité accessible sur son site internet[177].

Elles font ainsi en sorte de permettre aux personnes concernées de pouvoir joindre le DPO[178] et mentionnent donc : l'adresse postale du DPO, son téléphone, son adresse électronique, et tout autre moyen de communication éventuellement utilisé au sein de l'organisme concerné, tel qu'un formulaire en ligne.

(iii) L'indépendance du DPO

148. **Un DPO libre dans l'exercice de ses missions**. Le DPO désigné de chaque Enseigne ne reçoit aucune instruction en ce qui concerne l'exercice des missions qui lui incombent[179], et exerce ses fonctions et missions en toute indépendance[180]. Par exemple, le DPO de chaque Enseigne ne reçoit aucune directive[181] sur la nécessité de réaliser une analyse d'impact, ou sur les modalités pour traiter la demande de suppression de ses données personnelles par un client[182]. Chaque Enseigne garantit que le DPO est libre de ses opinions, y compris en cas de divergence avec celles des organes hiérarchiquement supérieurs travaillant au sein de l'Enseigne. Enfin, chaque Enseigne garantit que les rapports du DPO sont transmis au niveau le plus élevé de la direction générale de l'Enseigne avec lequel il établit un calendrier d'échanges réguliers[183].

---

[177] Si la publication du nom du DPO peut constituer une bonne pratique, il appartient au responsable du traitement, ou au sous-traitant, et au DPO de décider si elle est nécessaire ou utile dans les circonstances particulières du cas considéré.

[178] Il n'est pas obligatoire pour l'Enseigne de communiquer le nom du DPO, mais cela est conseillé afin de faciliter les missions de la CNIL et des employés de l'Enseigne. Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.12-13.

[179] Article 38 § 3 ; Considérant 97, RGPD.

[180] Considérant 97, RGPD.

[181] Ceci ne concerne toutefois pas les directives générales que l'Enseigne peut donner à ses employés, et qui s'appliquent également au DPO (par exemple une directive en matière d'hygiène et de sécurité).

[182] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.14.

[183] Article 38 § 6, RGPD.

(iv) <u>La prohibition des conflits d'intérêts</u>

149. Le DPO de chaque Enseigne peut se voir attribuer d'autres missions que celles attachées à sa fonction mais elles ne doivent en aucun cas entraîner de conflit d'intérêts[184].

<u>ILLUSTRATIONS PRATIQUES</u>

Le DPO peut :

- Être sollicité pour participer à des tâches liées aux obligations de l'Enseigne l'ayant désigné, à la condition que la décision revienne à l'Enseigne, en sa qualité de Responsable de Traitement ;
- Se voir confier la tenue matérielle du registre, dont le contenu reste toutefois sous la responsabilité de l'Enseigne[185] ;
- Cumuler cette fonction avec celle de responsable de la sécurité des systèmes d'information (RSSI) dès lors qu'il est dépourvu de pouvoir décisionnel sur la finalité et le moyen des Traitements.

Le DPO ne peut pas :

- Prendre une décision portant sur la création ou sur les conditions de mise en œuvre d'un traitement, notamment en concourant à la détermination des moyens ou des finalités de celui-ci. Par exemple, il ne peut pas mettre en place le traitement de gestion de programmes de fidélité dépendant des dates de naissance des Clients pour procéder à des opérations de campagnes de publicité ciblées en fonction de l'âge ;
- Endosser une fonction de décideur à côté de sa fonction de DPO, en raison de l'éventuel conflit d'intérêt pouvant survenir. Par exemple le DPO de l'Enseigne ne peut pas être son directeur opérationnel, financier voire juridique[186] dès lors qu'il s'agit de fonction qui sont susceptibles d'impliquer la détermination des moyens et des finalités des traitements ;
- Représenter le Responsable du Traitement ou le Sous-traitant devant une juridiction dans le cadre d'un litige portant sur la protection des données[187].

[184] Article 38 § 6, RGPD.

[185] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p. 22. Le DPO peut se voir assigner d'autres missions que celles attachées à son statut et résultant des articles 37 et 38 du RGPD ; toutefois, ces missions complémentaires ne doivent à aucun moment entrainer un « conflit d'intérêts » (article 38, §6 du RGPD), ce qui exclut que le DPO endosse une fonction de « décideur » (lignes directrices du G29 du 13 décembre 2016, p. 19). Aussi, les missions complémentaires du DPO devront se cantonner à des diligences purement matérielles, sans pouvoir décisionnaire, raison pour laquelle la tenue (matérielle) d'un registre peut être confiée au DPO (ce que le G29, désormais CEPD, a admis dans ses lignes directrices du 13 décembre 2016 à propos des DPO page 22).

[186] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.15.

[187] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.16.

150. **EXIGENCE AUDITABLE : ETABLIR LA VERIFICATION DES CRITERES INHERENTS A LA FONCTION DE DPO**. L'Enseigne s'engage à fournir la preuve qu'elle s'est assurée, au préalable, que les critères suivants soient bien remplis :

- Le DPO désigné est professionnellement compétent dans le domaine de la protection des données à caractère personnel et dans le secteur de la vente au détail d'équipements de la personne ;
- Le DPO dispose des qualités personnelles d'intégrité et d'éthique exigées pour exercer la fonction ;
- La désignation du DPO a bien été réalisée auprès de la CNIL, par exemple *via* le téléservice mis en ligne par la CNIL à cet effet ;
- Le DPO ne reçoit aucune instruction dans l'exercice de ses fonctions et il les exerce en toute indépendance ;
- Les missions exercées par le DPO en dehors de son strict statut n'entraînent aucun conflit d'intérêt avec sa fonction.

3.7.3. Les missions du DPO

151. **RAPPEL DE LA RÈGLE.** Les missions assignées au DPO par le RGPD sont les suivantes :

- Informer et conseiller l'Enseigne en sa qualité de Responsable de Traitement ou de Sous-traitant en matière de protection des données[188] ;
- Contrôler le respect des dispositions, issues du RGPD et de la loi « Informatique et Liberté » ou des règles de l'entreprises, applicables en matière de protection des données à caractère personnel[189] ;
- Coopérer et faire office de point de contact avec l'autorité de contrôle[190] ;
- Se tenir à la disposition des personnes concernées[191] pour répondre :
  - À toute question relative à l'exercice de leurs droits (accès, rectification, opposition, portabilité, limitation, effacement, droit de donner des directives après la mort), et
  - À toutes les questions relatives au Traitement de leurs données[192] ;
- Conseiller et vérifier l'exécution des analyses d'impact[193].

[188] Article 39 § 1, a), RGPD.
[189] Article 39 § 1, b), RGPD.
[190] Article 39 § 1, d) et e), RGPD.
[191] Les personnes concernées sont, conformément à l'**Annexe A3** : l'abonné, le client - classique, fidèle ou parrain -, le fournisseur, le prospect, le tiers parrainé-filleul, le vendeur, le visiteur et l'utilisateur.
[192] Article 83 § 4, RGPD.
[193] Article 39 § 1, c), RGPD.

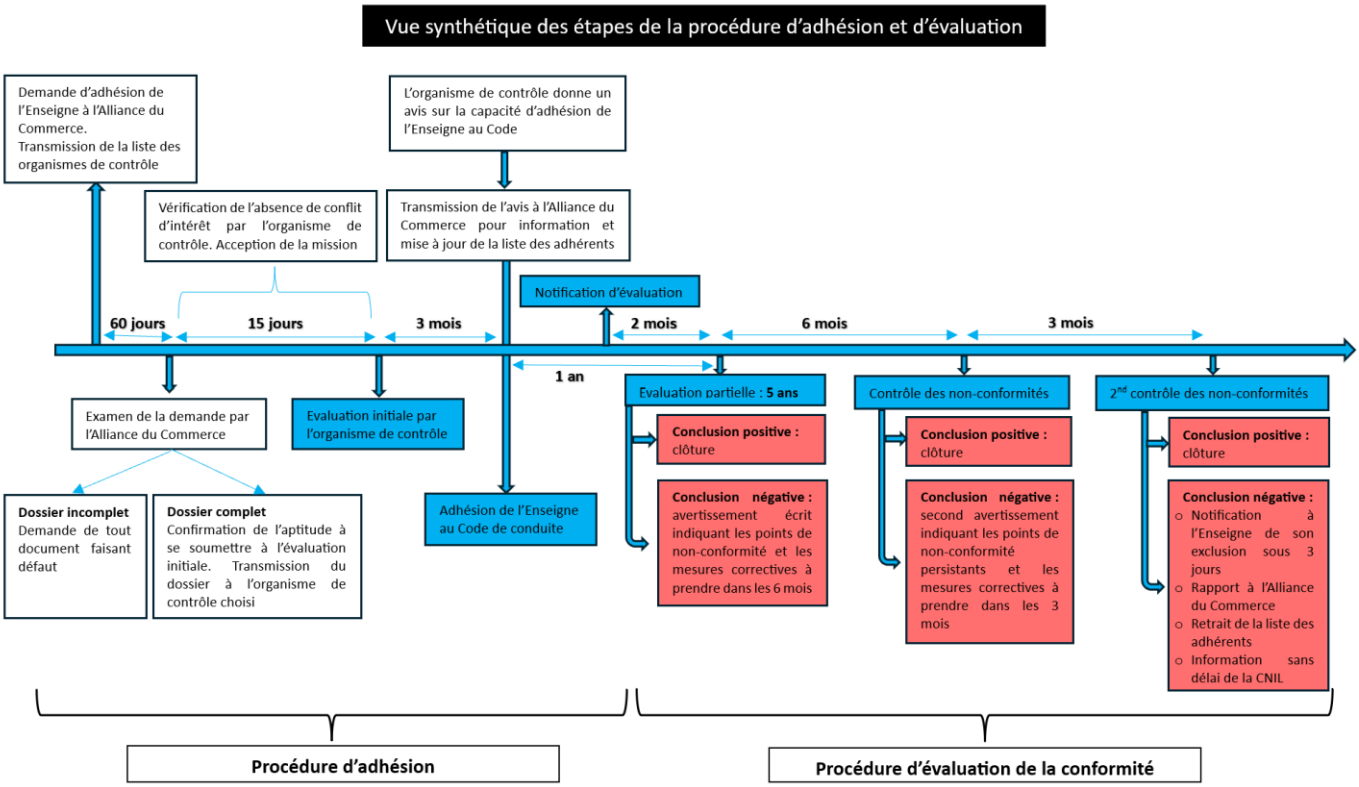
152. **TRADUCTION DE LA RÈGLE JURIDIQUE AU COMMERCE DE DÉTAIL**. De manière plus générale, le DPO désigné de chaque Enseigne est investi de deux rôles :

- Référent sur la conformité : le DPO identifie les traitements et dispense des conseils à l'Enseigne, la sensibilise sur les sujets de sa compétence et fait office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement[194]. Par exemple, il peut s'agir de la mise en place de mesures techniques et organisationnelles, dont la responsabilité reste néanmoins celle de l'Enseigne[195] ;
- Rôle particulier en matière d'analyse d'impact : le Responsable de Traitement a l'obligation de demander conseil au DPO avant la réalisation d'une analyse d'impact préalable[196], lequel sera chargé d'en vérifier l'exécution[197]. Il doit se prononcer sur (i) la nécessité de procéder ou non à une analyse d'impact, (ii) la méthodologie et les modalités de réalisation de cette analyse, (iii) la pertinence des mesures et garanties prévues pour remédier aux risques identifiés[198].

153. **EXIGENCE AUDITABLE : LA CLARIFICATION PRECISE DES MISSIONS DU DPO**. L'Enseigne s'engage à élaborer une fiche de poste du DPO détaillant les missions précises de ce dernier, précisant le caractère indépendant de l'exercice de sa fonction et lui octroie les moyens humains, matériels et financiers nécessaires à l'accomplissement de ses missions.

[194] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.16 ; Considérant 97, RGPD ; article 39, §1, b) et e) du RGPD.
[195] Article 24 § 1, RGPD.
[196] Article 35 § 2, RGPD.
[197] Article 39 § 1, c), RGPD.
[198] Lignes directrices adoptées par le G29 le 13 décembre 2016 à propos des DPO, p.17.

CHAPITRE 4 – GOUVERNANCE DU CODE



154. L'association, l'Alliance du Commerce, en sa qualité de Porteur du Code de conduite, est responsable de la gouvernance dudit Code.

155. La gouvernance du Code est répartie entre divers organes, pour certains considérés internes à l'Alliance du commerce, et pour d'autres externes au groupement :

4.0. Organes internes

- <u>Conseil d'administration de l'Alliance du Commerce</u>

156. L'Alliance du Commerce est gérée par un Conseil d'administration composé d'un ou plusieurs administrateurs, représentants personnes physiques des enseignes adhérentes, désignés par l'assemblée générale ordinaire des membres de l'association, conformément à l'article 9 de ses statuts.

157. **Missions**. Le Conseil d'administration a pour mission d'/ de :

- Examiner et actualiser l'adhésion des Enseignes au Code de conduite, et en communiquer à la CNIL, sous réserve du contrôle a *priori* et de l'avis contraignant de l'Organisme de contrôle ;

- Etablir et transmettre aux Enseignes la liste des organismes de contrôle agréés qui seront compétents pour contrôler la conformité des Enseignes aux dispositions du Code ;
- Approuver la désignation d'un représentant proposé par l'Enseigne pour intégrer le Groupe de travail sur le Code de conduite ;
- Proposer des modifications du Code de conduite ;
- Approuver les modifications présentées par le Groupe de travail, et adopter une résolution spéciale le cas échéant ;
- Définir et mettre à jour les directives d'utilisation de la marque de conformité.

- <u>Groupe de travail sur le Code de conduite</u>

158. **Composition**. Lors de son adhésion au Code de conduite, chaque Enseigne désigne au sein de son personnel un représentant chargé de présenter la déclaration d'adhésion, et qui endosse un rôle d'intermédiaire entre l'Organisme de contrôle et l'Enseigne. Le Groupe de travail se compose d'un nombre de représentants correspondant à un tiers du nombre d'Enseignes adhérentes, sans dépasser quinze (15) personnes représentatives choisies parmi les trois fédérations composant l'Alliance du Commerce (FEH, FEC et UCV[199]).

159. **Sélection**. Chaque Enseigne, après adhésion au Code de conduite, peut soumettre, à sa discrétion, le représentant ayant présenté la déclaration de conformité, conformément à la procédure visée au Chapitre 5 du présent Code, au Conseil d'administration de l'Alliance du Commerce, lequel est chargé d'accepter ou de motiver une décision de refus à la désignation de ce représentant pour intégrer le Groupe de travail.

160. **Expertise requise**. Ces représentants doivent nécessairement disposer d'une expertise en matière de protection des données, et occuper un poste stratégique en matière de vente au détail d'équipement de la personne susceptible de justifier d'une parfaite compréhension des attentes en matière RPGD dans le secteur (délégué à la protection des données, juriste, directeur financier / marketing, par exemple).

161. **Missions**. Les principales missions du Groupe de travail sont :

- Solliciter les organismes de contrôle, afin de recueillir leur retour pratique pour toute modification du Code de conduite ;
- Proposer, au Conseil d'administration, des modifications du Code en lien avec l'évolution des usages et/ou de la législation relative à la protection des données, conformément aux exigences prévues au Chapitre 8 du présent Code ;

[199] L'Alliance du Commerce est un groupement d'intérêt économique (GIE), constituée par trois associations :
- la Fédération des Enseignes de l'Habillement (FEH) ;
- la Fédération des Enseignes de la Chaussure (FEC) ;
- l'Union du Grand Commerce de Centre-ville (UCV).

- Proposer tout complément et/ou référentiel susceptible de faciliter le traitement des demandes des adhésions.

4.1. Organisme(s) de contrôles externes

162. **Désignation**. L'article 40.4 du RGPD prévoit qu'un organisme qui répond aux critères de l'article 41.1 est désigné pour procéder à des contrôles de la bonne application des dispositions du Code de conduite parmi les Enseignes qui y adhèrent. Conformément aux articles 40.4 et 41 du RGPD, le présent Code décrivent les mécanismes permettant à un organisme de contrôle, sélectionné par le Porteur du Code, de contrôler le respect du Code.

163. **Rappel pédagogique**. L'Organisme de contrôle dispose du niveau d'expertise approprié relativement au secteur concerné, pour lequel il doit recevoir un agrément par la CNIL[200]. La durée de l'agrément délivré par l'autorité de contrôle est fixée à cinq ans[201]. La démarche adoptée par l'Organisme de contrôle doit lui permettre de s'assurer que tous les traitements qu'il effectue dans le cadre de ses missions sont conformes aux dispositions du présent Code.

164. L'Alliance du Commerce tient à disposition une liste d'Organismes de contrôle sélectionnés par ses soins, agréés par la CNIL à l'issue d'une procédure d'agrément qu'ils doivent respecter.

4.1.1. Désignation, mandat et fonctionnement

165. **Choix de l'Organisme de contrôle par l'Enseigne**. Le représentant désigné de chaque Enseigne choisit l'Organisme de contrôle parmi la liste élaborée et tenue par l'Alliance du commerce. L'Organisme de contrôle, qui accepte cette désignation, s'engage par écrit, à respecter les dispositions du présent Code le concernant.

166. **Cas de cessation des fonctions**. L'Organisme de contrôle est choisi pour une durée de cinq ans[202] renouvelable et sans préjudice de l'exercice à tout moment des compétences de la CNIL au regard des obligations de cet organisme de contrôle (issues de la délibération 2020 – adoption d'un référentiel agrément[203]). Les missions de cet organisme de contrôle peuvent toutefois prendre fin avant ce terme dans les cas suivants :

- Retrait ou révocation de l'agrément qui sera notifiée par tout moyen aux Enseignes concernées afin qu'elles puissent sélectionner un nouvel organisme qui prendra la suite des missions réalisées par son prédécesseur ;

[200] CNIL, Délibération N°2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite

[201] CNIL, Délibération N°2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite

[202] Cette durée est alignée sur la délivrance et le renouvellement de l'agrément par la CNIL.

[203] CNIL, Délibérationn° 2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite

- A la demande de l'Organisme de contrôle ;
- A l'initiative d'une Enseigne qui décide de se désengager du Code de conduite ;
- A l'issue d'une procédure de sanction prononcée contre une Enseigne pour non-conformité. Dans ce cas, la résiliation prendra effet à la date de notification de la décision d'exclusion.

Conséquences du retrait d'agrément. Au terme de l'agrément ou en cas de révocation :
- L'organisme de contrôle s'engage à transmettre toute documentation et informations aux nouveaux Organismes de contrôles choisis par les enseignes concernées,
- Cette communication est effectuée sans délai et au plus tard dans le délai d'un mois à compter du terme de l'agrément ou de sa révocation et sans coûts additionnels.

167. **Cas du refus de mission.** L'Organisme de contrôle conserve la faculté de refuser d'agir pour une Enseigne qui l'aurait désigné, même en l'absence de conflit d'intérêts.

Dans l'hypothèse où un différend de quelque nature que ce soit naît entre un Organisme de contrôle et une Enseigne, l'Alliance du commerce organise une médiation entre les deux parties, afin de tenter de trouver une solution et résoudre le désaccord.

168. **Missions**. Les principales responsabilités de l'Organisme[204] sont les suivantes :

- Rendre un avis contraignant sur la capacité d'adhésion des Enseignes au Code de conduite ;
- Procéder à une évaluation initiale de conformité, effectuée préalablement à l'adhésion des Enseignes au Code[205] ;
- Contrôler régulièrement la conformité des Enseignes au Code, selon une périodicité établie conformément aux exigences d'évaluation de conformité du présent code[206] ;
- Exprimer un avis non contraignant sur les propositions de modifications du Code présentées par le Groupe de travail après approbation par le Conseil d'administration ;
- Solliciter une révision du Code de conduite ;
- Examiner les plaintes relatives à la non-conformité au Code et tenir un registre des plaintes ;
- Effectuer des évaluations et/ou des vérifications des points persistants de non-conformité d'une Enseigne visée par une plainte ou jugée non conforme à l'issue du contrôle de conformité réalisé ;
- Imposer des mesures contraignantes à l'encontre d'une Enseigne non conforme, en informer le Conseil d'administration et permettre à la CNIL de pouvoir y accéder ;
- Présenter ses rapports de synthèse au Conseil d'administration et les mettre à la disposition de la CNIL ;

[204] Délibération n°2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite

[205] Evaluation initiale effectuée dans les termes prévus au « (i) Evaluation de la conformité au Code ».

[206] Evaluation annuelle effectuée dans les termes prévus au « (i) Evaluation de la conformité au Code ».

- Signaler à la CNIL toute problématique (autre qu'une décision contraignante) qu'il jugerait nécessaire en lien avec l'application du Code.

4.1.2. Critères de sélection de l'Organisme de contrôle

169. **Des organismes sélectionnés à l'issue d'un appel d'offres**. Le Conseil d'administration de l'Alliance du Commerce établit une liste d'organisations externes indépendantes, sélectionnées à l'issue d'un processus d'appel d'offres[207], et sous condition suspensive de l'obtention de l'agrément délivré par la CNIL, ou le cas échéant son renouvellement. Chacune de ces organisations doit faire la démonstration qu'elle remplit les critères énoncés par la CNIL dans la Délibération N°2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite.

(v) Le critère d'indépendance

170. **Démonstration des capacités**. L'Organisme de contrôle remplit le critère d'indépendance, vis-à-vis de l'Alliance du Commerce, des Enseignes adhérentes, et des professionnels du secteur de la vente au détail d'équipements de la personne. L'Organisme de contrôle apporte tous les justificatifs pertinents (code de déontologie par exemple) permettant de garantir ses capacités, dans la procédure d'agrément mise en place en vue de sa désignation, son mandat et son fonctionnement.

171. **Des ressources nécessaires**. Afin de démontrer son indépendance fonctionnelle, l'Organisme de contrôle dispose des ressources humaines et techniques nécessaires à l'exécution de ses tâches. Elle se démontre notamment grâce à la procédure de recrutement du personnel, la rémunération de ce dernier, la durée des missions et des contrats[208].

172. **Indépendance financière**. Afin de démontrer son indépendance financière, l'Organisme de contrôle dispose d'un financement adapté et d'une viabilité financière suffisants pour l'accomplissement de ses missions, qu'il peut notamment justifier par l'allocation d'un budget spécifique destiné à l'accomplissement de ses missions.

173. **Indépendance décisionnelle**. Afin de démontrer son indépendance décisionnelle, l'Organisme de contrôle doit prouver qu'il est seul décisionnaire dans le cadre de ses activités, par le biais de tout document pertinent. Il est parfaitement libre dans sa prise de décision, et ses décisions ne sont soumises à aucune approbation de la part d'un autre organisme, ni de l'Alliance du Commerce, ni d'une Enseigne adhérente. Toutefois, les refus qu'il oppose doivent être motivés.

[207] Etant précisé que l'appel d'offres prévoit un prérequis relatif au respect du RGPD par l'entité qui souhaite candidater pour être nommé organisme de contrôle. Ce prérequis porte uniquement sur les missions d'audit de l'entité.

[208] Exemples de documentation à fournir à l'appui d'une demande d'agrément – Agrément des organismes chargés de contrôler le respect des codes de conduite (Délibération n°2020-050 du 30 avril 2020)

(vi) Le critère de l'absence de conflits d'intérêts

174. **La mise en place de process permettant de prévenir la survenance de tout conflit d'intérêt**. L'Organisme de contrôle n'est sollicité, ni ne reçoit d'instructions d'aucune autre personne physique ou morale, d'organisations ou d'associations. L'Organisme de contrôle met en place les procédures et les mesures afin d'éviter tout conflit d'intérêts et rester libre de toute influence externe et interne, et de se prémunir contre toute action incompatible avec ses missions. A cet effet, il dispose d'une procédure interne spécifique, et de modèles adaptés permettant de prévenir et/ou déclarer, ainsi que, le cas échéant, de traiter un conflit d'intérêt dans les relations entre son personnel et ses Sous-traitants, à l'égard du Porteur du Code, des adhérents et de tout autre organisme.

175. **La procédure en cas de conflit d'intérêt**. Dans l'hypothèse où un conflit d'intérêts apparaît, c'est-à-dire que l'Enseigne a fait le choix d'un organisme de contrôle, dont la procédure de prévention des conflits ne permet pas de garantir l'impartialité de ce dernier, l'Organisme de contrôle suivra la procédure suivante :

- L'Organisme de contrôle désigné doit informer concomitamment le représentant de l'Enseigne concernée et le Groupe de travail de la situation de conflit ;
- Lorsque le Groupe de travail atteste par écrit – par courrier électronique – de la situation de conflit d'intérêt, il doit proposer un organisme remplaçant à l'Enseigne concernée ;
- L'Organisme de contrôle concerné doit se retirer automatiquement du Groupe de travail ;
- S'il ne se retire pas à l'issue d'un délai de vingt-et-un (21) jours à compter de la demande du Groupe de travail, le Groupe de travail en réfère au Conseil d'administration de l'Alliance du Commerce qui le raye de la liste des organismes de contrôle.

(vii) Le critère afférent à l'expertise

176. **Les facteurs pris en considération**. L'Organisme de contrôle doit démontrer une expertise spécifique dans le secteur concerné et une expérience significative précise. Les facteurs pris en compte dans l'évaluation de ces compétences sont :

- Sa connaissance du secteur concerné, c'est-à-dire le secteur de la vente au détail d'équipements de la personne ;
- Sa maitrise des risques liés aux activités de traitement propre à la vente du détail d'équipement de la personne ;

L'Organisme de contrôle peut justifier de ces compétences à l'aide des procédures de recrutement qu'il met en place et des descriptions de poste qu'il propose.

177. **Un personnel bipartite**. Chaque Organisme de contrôle agréé dispose d'un personnel de direction chargé du processus décisionnel, d'une part, et d'un personnel chargé d'exécuter

le contrôle des Enseignes[209]. Dans l'accomplissement de ses missions, l'Organisme de contrôle sélectionné peut sous-traiter[210] l'exécution du contrôle des Enseignes à un tiers, dès lors qu'il reste le référent responsable des décisions finales.

178. **Le processus décisionnel**. S'agissant du personnel de direction chargé du processus décisionnel, l'Organisme fixe les règles d'évaluation des connaissances et des compétences de son personnel. L'organisme de contrôle dispose d'une équipe possédant une expérience approfondie et significative des questions et des enjeux relatifs aux données personnelles, au secteur de la vente au détail d'équipements de la personne, ainsi que dans la compréhension des modèles commerciaux dans le secteur de la vente physique et du e-commerce[211].

179. **Le processus de contrôle**. S'agissant du personnel exerçant les activités de contrôle, l'Organisme de contrôle dispose d'une équipe disposant collectivement d'une expertise appropriée[212] et significative dans le domaine de la vente au détail d'équipements de la personne, en matière de protection des données et dans la compréhension des modèles commerciaux dans le secteur de la vente physique et du e-commerce.

4.2. Contrôle du respect du code

4.2.1. Contrôles réguliers, complets et transparents

180. **Rémunération de l'Organisme de contrôle**. L'Enseigne rémunère l'Organisme de contrôle désigné pour toutes les activités qu'il exerce dans le cadre de ses missions du respect du Code. La rémunération versée à l'Organisme par l'Enseigne ne saurait remettre en cause l'indépendance de ce dernier. Le barème de rémunération de l'Organisme de contrôle, validé par l'Alliance du Commerce, est déterminé au moment de son agrément par la CNIL.

4.2.2. Modalités de contrôle du respect du Code

(i) Evaluation de la conformité au Code

181. **Evaluation initiale**. Une évaluation initiale de conformité à l'ensemble des exigences du Code est effectuée sans délai à l'issue de la sélection de l'Organisme par l'enseigne souhaitant adhérer au Code, au regard de la documentation fournie par l'Enseigne lors de sa demande d'adhésion (cf. Chapitre 5, 2.). A l'issue de cette évaluation :

[209] Exemples de documentation à fournir à l'appui d'une demande d'agrément – Agrément des organismes chargés de contrôler le respect des codes de conduite (Délibération n°2020-050 du 30 avril 2020)

[210] En cas de sous-traitance, l'organisme de contrôle reste responsable des décisions finales.

[211] Conformément aux exigences de la Délibération N°2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite en matière d'expertise juridique et technique.

[212] Conformément aux exigences de la Délibération N°2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite en matière d'expertise juridique et technique.

- L'Organisme confirme la conformité au code de l'Enseigne ainsi que son adhésion au Code,
- Dans l'hypothèse où l'Organisme n'est pas en mesure de confirmer la conformité de l'Enseigne, il peut dresser un état des lieux qu'il adresse à l'Enseigne concernée. Ce document confidentiel permet à l'Enseigne de connaître les points d'amélioration qu'elle doit mettre en œuvre. Une seconde évaluation pourra avoir lieu, étant précisé que l'enseigne souhaitant adhérer au Code de conduite ne sera considérée comme adhérente officielle qu'une fois les exigences de l'Organisme de contrôle satisfaites,
- L'Organisme refuse l'adhésion s'il établit que l'Enseigne n'est conforme à aucune des exigences du Code à l'issue de l'évaluation initiale et qu'une seconde évaluation n'aurait pas d'utilité, ou dans le cas où à l'issue de la seconde évaluation la conformité de l'Enseigne au code n'est toujours pas établie. Dans les deux cas, il doit motiver sa décision de refus.

182. **Evaluation annuelle.** Lors des vérifications de conformité annuelles opérées, l'Organisme de contrôle procède à un audit périodique sur les exigences du Code prises isolément et annuellement sans ordre prédéterminé mais selon la nomenclature suivante :

- Consentement et information des personnes concernées, conformément aux exigences posées au Chapitre 2 et au 3.1. ;
- Procédure d'exercice des droits des personnes concernées conformément aux exigences posées au 3.2. ;
- Encadrement des contrats et Transferts hors Union Européenne, conformément aux exigences posées aux 3.3. et 3.4. ;
- Obligation de sécurité, conformément aux exigences posées au 3.5. ;
- Registre des traitements et Délégué à la protection des données personnelles, conformément aux exigences posées au 3.6. et 3.7.
- Une fois la procédure de contrôle initiale passée, l'Organisme de contrôle désigné vérifie la conformité de chaque Enseigne qui l'a désigné à certaines exigences du Code représentant annuellement au moins 20% des exigences totale du Code, et donnant lieu à un rapport quinquennal qui consolidera le rapport annuel élaboré à l'issue de chaque contrôle.
- L'Enseigne est informée du contrôle deux (2) mois au préalable, afin de lui permettre de réunir la documentation nécessaire au contrôle.

183. **Rédaction d'un rapport d'audit**. Ces audits approfondis de conformité feront l'objet d'un rapport écrit à l'issue de l'entier contrôle du Code de conduite, qui rassemblera l'ensemble des rapports rédigés à l'issue de chaque contrôle. Ce rapport sera présenté au Conseil d'administration – afin de lui permettre d'en prendre connaissance notamment en cas de procédure de sanction – et mis à disposition de la CNIL.

(ii) Démonstration des résultats

184. **La retranscription des résultats constatés**. A l'issue de chaque audit approfondi, l'Organisme de contrôle procède à la rédaction d'un rapport, retranscrivant la procédure mise en œuvre par ses soins dans le cadre du contrôle et ses résultats. Chaque résultat exposé est accompagné d'une conclusion et d'un constat de conformité aux dispositions du Code.

185. **Des décisions motivées**. Lorsqu'il souhaite prendre une décision, l'Organisme de contrôle, doit la motiver, en exposant les motifs la justifiant, à la lumière des éléments de contrôle l'ayant conduit à prendre une décision et en se référant au Code de conduite. L'Organisme de contrôle peut formuler toute demande d'informations et/ou de précisions auprès de l'Enseigne contrôlée, qui s'engage à lui fournir dans un délai raisonnable fixé par l'Organisme selon la nature et la quantité des éléments à réunir.

186. **La communication du/des rapport(s)**. L'Organisme de contrôle adresse un premier rapport d'audit à l'Enseigne concernée dans un délai de trois (3) mois à l'issue des opérations de contrôle retracées dans un rapport exhaustif à l'issue d'une période de cinq ans, lorsqu'il a contrôlé l'Enseigne sur le respect de l'intégralité du Code[213].

(iii) Traitement des plaintes

187. **Un process permettant la prévention des violations du Code**. L'Organisme de contrôle élabore une procédure de traitement impartial et objectif des plaintes concernant les violations du Code ou la manière dont le Code est appliqué par une Enseigne adhérente. Toute personne concernée a qualité pour déposer une plainte.

188. **La mise en place d'une procédure de gestion des plaintes**. L'Organisme de contrôle met en place une procédure de gestion des plaintes accessible sur son site internet. A réception d'une plainte, l'Organisme informe le plaignant du délai de traitement de sa plainte, laquelle ne peut excéder un (1) mois à compter de sa réception. Le délai peut être prorogé de deux (2) mois, si la plainte se révèle d'une complexité suffisante empêchant l'Organisme de la traiter dans un délai inférieur. Dans l'hypothèse où la plainte est adressée directement à l'Alliance du Commerce, cette dernière se chargera de la rediriger vers l'Organisme concerné.

189. **La tenue d'un registre des plaintes**. L'Organisme de contrôle tient à jour un registre des plaintes, qu'il tient à la disposition de l'autorité de contrôle qui peut y accéder à tout moment. Ce registre doit présenter exhaustivement la nature de chaque plainte, l'identité du plaignant (personne concernée ou Enseigne adhérente), le délai de traitement et les motifs de la décision prise avant la clôture de la plainte[214]. Il transmet au personnel permanent de l'Alliance du Commerce, des informations statistiques générales concernant le nombre et le type de plaintes/infractions et les résolutions/mesures correctives émises.

[213] Cf. 4.3. Information de l'autorité de contrôle

[214] Exemples de documentation à fournir à l'appui d'une demande d'agrément – Agrément des organismes chargés de contrôler le respect des codes de conduite (Délibération n°2020-050 du 30 avril 2020)

(iv) Procédure de sanction

190. L'Organisme de contrôle qui, au cours du processus de traitement d'une plainte ou à l'issue du contrôle de conformité réalisé chaque année ou au terme des cinq ans, constate que l'Enseigne concernée n'est pas conforme aux dispositions du Code de conduite, met en place les mesures suivantes :

- **Première étape** : il adresse un avertissement écrit par courrier électronique à l'Enseigne, et lui expose :

- Les points de non-conformité, accompagnés des conclusions y afférentes que l'organisme de contrôle a dégagées ;
- Les mesures correctives devant être prises par l'Enseigne et le délai de six (6) mois pour les mettre en place ;
- La mention selon laquelle à défaut de mettre en place ces mesures dans le délai imparti, l'Enseigne s'expose à la publication d'un constat de non-conformité à son encontre.

A l'issue du délai précité, l'Organisme de contrôle procède à un nouveau contrôle de vérification du respect des exigences du Code sur les points précités, au cours duquel l'Enseigne s'engage à fournir tout document utile (preuves, observations) de nature à démontrer sa conformité. Lors de cette seconde évaluation,

- Si l'Organisme conclut positivement, c'est-à-dire qu'il constate que l'Enseigne a remédié à sa non-conformité, il clôt la procédure ;
- Si l'Organisme conclut négativement, c'est-à-dire qu'il constate que l'Enseigne demeure non-conforme au Code de conduite, il lui adresse un second avertissement par courrier électronique.

- **Deuxième étape** : le second avertissement écrit expose :

- Les points persistants de non-conformité à l'issue des deux premières évaluations, ainsi que les motifs qui ont conduit l'Organisme à conclure à l'insuffisance des mesures prises ;
- Les mesures correctives à mettre en place par l'Enseigne et le délai de trois (3) mois lui étant imparti ;
- La mention de la décision prise par l'organisme de contrôle de suspendre ou non l'adhésion de l'Enseigne concernée si elle ne remédie pas à la non-conformité. En cas de suspension, il informe sans délai la CNIL sans omettre de préciser les raisons justifiant cette mesure ;
- La mention selon laquelle le défaut persistant de conformité entraînera le retrait de l'Enseigne de la liste des adhérents au Code de conduite sur le site du Porteur du Code ainsi que l'interdiction d'usage de la marque de conformité.

- **Troisième étape** : à l'issue du délai précité, l'Organisme de contrôle réitère son évaluation du respect des exigences du code sur les points précités. Lors de cette troisième évaluation, en cas de persistance de non-conformité, cet organisme :

- Notifie, par voie électronique, à l'Enseigne concernée son exclusion du bénéfice du présent Code, dans un délai de trois (3) jours à compter de l'achèvement de l'évaluation ;

- Informe dans les mêmes délais l'Alliance du Commerce qui s'engage à alerter le Groupe de travail et à retirer l'Enseigne concernée de la liste des adhérents au Code sur son site internet, ;
- Informe sans délai la CNIL de la décision d'exclusion sans omettre d'inclure les raisons justifiant cette mesure.

191. **Une possibilité de contestation**. A toute étape du déroulement de la procédure de sanction ci-dessus, l'Enseigne visée conserve la possibilité de contester les conclusions de l'Organisme en faisant valoir des observations qu'elle documente.

192. Toute nouvelle demande d'adhésion formulée par l'Enseigne doit préciser la circonstance préalable d'exclusion et est soumise à un contrôle minutieux de l'organisme. Son acceptation est conditionnée à la démonstration de conformité en tous points aux exigences du code[215].

4.3. Information de l'autorité de contrôle compétente

4.3.1. Rapports de synthèse

193. **Un rapport annuel et un rapport quinquennal**. L'Organisme de contrôle informe l'Alliance du Commerce à l'issue de l'évaluation initiale pour lui faire part du résultat de celle-ci. Il formalise l'ensemble des rapports annuels dans un rapport exhaustif à l'issue d'une période de cinq ans, lorsqu'il a contrôlé l'Enseigne sur le respect de l'intégralité des dispositions du Code[216], et transmet pour information une synthèse à l'Alliance du Commerce.

194. **Contenu du rapport**. Le rapport de synthèse quinquennal consolidant les cinq audits annuels sont tenus à la disposition de la CNIL. Le rapport détaille, de manière non exhaustive :

- Les méthodologies de contrôle et d'audit ;
- Le registre des plaintes tenu par l'organisme ;
- Un bilan des missions accomplies par l'organisme ;
- Les mesures prises à l'encontre des Enseignes ;
- Les points d'amélioration dans l'accomplissement de ses tâches.

4.3.2. Rapport spécifique en cas de mesure prise à l'encontre d'une Enseigne

195. Lorsque l'Organisme de contrôle décide d'une mesure coercitive à l'encontre d'une Enseigne, il permet à la CNIL d'avoir accès à sa décision et la lui communique sans délai, conformément à la section « (iv) Procédure de sanction » décrite précédemment.

[215] Sauf demande expressément motivée par l'Enseigne, l'organisme de contrôle à l'origine de la première procédure est celui en charge du nouveau contrôle, étant précisé que la circonstance selon laquelle l'organisme a déjà sanctionné l'Enseigne ne saurait justifier quelconque demande de cette dernière de changer d'organisme de contrôle.

[216] Cf. 4.3. Information de l'autorité de contrôle

4.4. Délais

196. A défaut de précision contraire, tous les délais exprimés dans le présent Code s'entendent en jours ouvrés, à savoir du lundi au vendredi inclus, hors jours fériés.

CHAPITRE 5 – DECLARATION DE CONFORMITE

197. Afin d'adhérer au présent Code, l'Enseigne doit être membre de l'Alliance du commerce et devra s'engager à se conformer à toutes les exigences du Code.

5.1. Processus d'adhésion au Code

198. L'Enseigne, souhaitant adhérer au Code, devra se soumettre à la procédure d'adhésion sous le contrôle de l'organisme de contrôle et remplir un formulaire d'adhésion.

199. **Etape préalable : évaluation initiale de conformité**. Une Enseigne souhaitant adhérer au Code est soumise à une évaluation initiale de conformité (évoquée au 4.2.2. du présent Code) par l'Organisme de contrôle avant de pouvoir présenter sa déclaration d'adhésion, qui sera vérifiée par le Conseil d'administration.

200. **Déroulement de la procédure**. Cette procédure d'adhésion se déroule de la manière suivante :

a) L'Enseigne présente sa demande d'adhésion au Conseil d'administration qui en accusera réception et lui transmettra aussitôt la liste des organismes de suivi agréés parmi lesquels l'Enseigne devra sélectionner celui qui sera chargé de son contrôle ;

b) Le Conseil d'administration examinera ensuite, et dans un délai de soixante (60) jours calendaires à compter de la réception de la demande, le dossier d'adhésion de l'Enseigne de façon à s'assurer que les documents pertinents sont complets :

   - En cas de dossier incomplet, le Conseil d'administration pourra solliciter tout document ou information manquant nécessaire auprès de l'Enseigne ;

   - En cas de dossier complet, le Conseil d'administration confirmera à l'Enseigne concernée son aptitude à se soumettre à l'évaluation initiale, laquelle pourra alors transmettre l'entier dossier à l'Organisme de contrôle qu'elle aura choisi.

c) Dans un délai de quinze (15) jours calendaires après réception du dossier, l'Organisme de contrôle choisi par l'Enseigne, procède aux vérifications de prévention de conflits d'intérêts, et confirme son acceptation de procéder à la mission ;

d) A l'issue du délai précité, l'Organisme de contrôle procède à l'évaluation initiale de la conformité de l'Enseigne au regard des exigences du Code, en remettant un rapport au plus tard dans un délai de trois (3) mois calendaires ;

e) A l'issue de cette évaluation, l'Organisme de contrôle transmet une copie de cette évaluation initiale au Conseil d'administration pour simple information et la complète d'un avis confidentiel contraignant sur la capacité d'adhésion et d'admission de l'Enseigne concernée à adhérer au Code ;

f) A la lumière de cet avis contraignant de l'Organisme de contrôle, l'Enseigne confirme ou non sa volonté d'adhérer directement auprès du Conseil d'administration ;

g) Le cas échéant, le Conseil d'administration actualise alors la liste des adhérents au Code de conduite, dans les quinze (15) jours. Cette liste est publiée sur son site internet, librement accessible au public.

201. Une fois officiellement inscrite sur la liste et déclarée adhérente, l'Enseigne est autorisée à utiliser la marque de conformité, comme indiqué à la section ci-dessous.

202. **Formulaire d'adhésion.** L'Enseigne devra renseigner exhaustivement les champs dans le formulaire figurant à l'**Annexe D**, et le transmettre au Conseil d'administration par courrier électronique. Le formulaire d'adhésion sera publié sur le site de l'Alliance du commerce et pourra y être mis à jour à tout moment.

5.2. Documentation

La démonstration de l'état d'avancement de mise en conformité. Lorsqu'elle se soumet à la procédure d'adhésion contrôlée[217], l'Enseigne doit être en mesure de démontrer l'état d'avancement de sa mise en conformité au Code de conduite.
A cette fin, elle est tenue de communiquer tous les documents justificatifs démontrant sa conformité aux exigences du Code[218]. Ces documents peuvent être utilisés, à la seule discrétion de l'Organisme de contrôle, afin d'évaluer le niveau de conformité de l'Enseigne. Par ailleurs, des documents ou informations supplémentaires peuvent être demandés par l'Organisme de contrôle chargé de vérifier la conformité.

5.3. Marque de conformité

203. **Un symbole public d'adhésion au Code de conduite**. Les Enseignes qui ont été déclarées conformes au Code sont autorisées à utiliser la marque de conformité (ci-après « **la Marque** ») élaborée et déposée par l'Alliance du Commerce, telle que figurant en **Annexe E**. La Marque sera utilisée comme symbole public de l'adhésion de l'Enseigne au Code de conduite.

204. **Un usage encadré**. Le Conseil d'administration définit et maintient à jour le règlement d'usage de la Marque, énonçant ses directives d'utilisation. L'Enseigne utilise la Marque exclusivement pour afficher son adhésion au Code et démontrer qu'elle respecte les exigences de conformité prévues par ce dernier. L'Enseigne sera autorisée à utiliser la Marque *a minima* sur son site internet, et conformément aux supports prévus au sein du règlement d'usage, tant que son adhésion reste valide, et qu'elle respecte le règlement d'usage accessible sur le site internet de l'Alliance du Commerce. Toute Enseigne ayant reçu une autorisation pour utiliser

[217] La procédure d'adhésion contrôlée correspond à la procédure d'évaluation initiale de conformité réalisée sous le contrôle de l'Organisme de contrôle.
[218] Il peut s'agir par exemple des politiques et procédures internes de l'Enseigne, des contrats avec les sous-traitants, des contrats de travail relatifs au personnel de l'Enseigne, des informations sur les politiques de confidentialité et de sécurité.

la Marque ne peut en céder l'usage à aucune autre Enseigne adhérente ou non, quel qu'en soit la forme ou le support.

CHAPITRE 6 – RETRAIT D'ADHESION

205. Si, dans le cadre d'une plainte ou d'un rapport annuel, l'Organisme de contrôle constate qu'une Enseigne n'a pas respecté les dispositions du Code, il devra suivre la procédure de sanction décrite au Chapitre 4 afin de déterminer la mesure corrective appropriée.

206. Ces mesures peuvent inclure la suspension et/ou le retrait d'adhésion de l'Enseigne lorsque, lors de sa troisième évaluation, l'Organisme constate que l'Enseigne persiste à demeurer non-conforme au Code de conduite.

207. **Procédure de retrait d'adhésion.** Afin d'exclure définitivement l'Enseigne de l'application du Code, l'Organisme de contrôle, après avoir constaté la non-conformité persistante de l'Enseigne[219] :

- Notifie, par voie électronique, à l'Enseigne concernée son exclusion du bénéfice du présent Code, dans un délai de trois (3) jours à compter de l'achèvement de l'évaluation ;
- En fait rapport dans les mêmes délais à l'Alliance du Commerce qui s'engage à en informer le Groupe de travail et à retirer l'Enseigne concernée de la liste des adhérents au Code sur son site internet, ;
- Informe sans délai la CNIL de la décision d'exclusion sans omettre d'inclure les raisons justifiant cette mesure.

208. **L'information de l'Enseigne**. L'Organisme de contrôle veille à ce que les droits de l'Enseigne soient respectés lors du processus de retrait d'adhésion. A cette fin, il communique les motifs du retrait à l'Enseigne concernée, qui conserve la possibilité de les contester par des observations qu'elle communique auprès de l'organisme jusqu'au prononcé du retrait de l'adhésion.

209. **Conséquences du retrait d'adhésion.** L'Enseigne, dont le retrait d'adhésion a été définitivement prononcé, perd le bénéfice d'utilisation de la Marque, telle que définie au Chapitre 5.3. du présent Code. Dans les trois (3) jours suivant la notification d'exclusion, l'Alliance du Commerce retire la référence à l'Enseigne concernée de la liste des adhérents figurant sur son site Internet et s'assure du retrait de la Marque du site de l'Enseigne et la cessation de son utilisation.

[219] Ainsi qu'il est précisé au sein de la « Troisième étape » de la procédure de sanction (iv) au sein du Chapitre 4.

CHAPITRE 7 – COMMUNICATION ET PUBLICATION DU CODE

210. **Publication du Code**. Postérieurement à l'approbation du Code par la CNIL, en sa qualité d'autorité de contrôle désignée, celle-ci enregistre et publie le Code par une délibération publiée sur son site Internet et par tout autre méthode de communication appropriée.[220]

211. Conformément à l'article 40.11 du RGPD, le Comité Européen à la Protection des Données (CEPD) intègre le Code de conduite approuvé au sein d'un registre répertoriant tous les codes de conduite précédemment approuvés. La version intégrale du Code est également publiée par l'Alliance du Commerce sur son site internet.

212. **Communication grâce à la Marque**. La Marque, prévue au 5.3., est destinée à permettre aux Enseignes adhérentes au Code de procéder à une communication unifiée. Toute communication par un autre biais que celui porté par la Marque est interdite, sauf autorisation expresse écrite délivrée par le Conseil d'administration.

213. L'usage de la Marque est conditionné par la stricte reproduction du logo tel qu'il aura été déposé par l'Alliance du commerce. La communication effectuée grâce à la Marque, qui exprime l'engagement de l'Enseigne de respecter les exigences du présent Code, ne saurait signifier une conformité au RGPD.

214. **Communication de l'Alliance du Commerce avec la CNIL**. Le Conseil d'administration enverra une communication à la CNIL une fois par an, identifiant les nouvelles Enseignes déclarées conformes au Code et les Enseignes exclues du bénéfice du Code au cours des douze derniers mois.

215. **Communication de l'Organisme de contrôle avec la CNIL**, chaque Organisme de contrôle communique régulièrement avec la CNIL dans les conditions exposées au Chapitre 4 du présent Code et dans les conditions définies par le référentiel d'agrément adopté par la CNIL.

[220] Lignes directrices adoptées par le CEPD le 4 juin 2019, à propos des codes de conduite, page 27.

CHAPITRE 8 – MODIFICATION DU CODE

216. L'Alliance du Commerce est tenue de réviser et modifier le Code en fonction des évolutions de la législation applicable en matière de protection des données à caractère personnel, et en particulier concernant le secteur de la vente et la distribution au détail de produits d'équipements de la personne.

217. La CNIL, en sa qualité d'autorité de contrôle compétente, approuve également toute modification ou prorogation du Code[221].

218. **Mise à jour du Code de conduite**. Le Groupe de Travail peut réviser le Code régulièrement afin de prendre en compte les évolutions juridiques et technologiques, ainsi que les meilleurs pratiques applicables au secteur concerné. A cet effet, il peut solliciter les Organismes de contrôle, afin de recueillir tout retour pratique pertinente en vue d'une modification du Code de conduite.

219. Le Conseil d'administration peut également initier à tout moment une telle révision par le Groupe de Travail, notamment si elle a été sollicitée par la CNIL ou par un organisme de contrôle.

220. Toute évaluation du Code n'entraîne pas nécessairement de proposition de modification, mais si tel est le cas, les propositions du Groupe de Travail devront être examinées et éventuellement adoptées comme il suit.

221. **Modifications du Code de conduite**. Après examen, s'il apparaît que des modifications du Code sont nécessaires, le Groupe de Travail doit proposer ses projets de modifications au Conseil d'administration. Pour être adoptée, toute modification du Code devra être :

- Présentée et approuvée par le Conseil d'administration ;
- Présentée aux organismes de contrôle choisis par les Enseignes, qui pourront prononcer un avis non contraignant formulé après échange avec ces dernières ;
- Présentée et examinée par la CNIL qui se prononce sur la question de savoir si la modification est ou non substantielle et entraîne un nouveau processus d'approbation.

Après approbation par l'autorité de contrôle, toute modification ou extension du Code est adoptée par le Conseil d'administration par une résolution spéciale qui devra intervenir dans les meilleurs délais. La version actualisée du Code devra être publiée par l'Alliance du commerce sur son site et son registre public.

222. **Renouvellement d'adhésion**. Les Enseignes devront également renouveler leur Déclaration d'adhésion dans les six (6) mois suivant la publication de la version actualisée du Code, sans avoir à subir un nouvel audit pour obtenir une nouvelle approbation en l'absence d'une modification substantielle du Code de conduite. En cas de modification substantielle une nouvelle évaluation sera réalisée par l'organisme de contrôle.

[221] Lignes directrices adoptées par le CEPD le 4 juin 2019, à propos des codes de conduite, page 28.