

Les réseaux de franchise et la protection des données à caractère personnel

Bien qu'entré en vigueur le 25 mai 2018, la conformité au Règlement Général sur la Protection des Données (« RGPD » ou « GDPR » en Anglais) reste toujours un défi à relever pour beaucoup d'entreprises, en particulier les réseaux de franchise. En effet, ce partenariat commercial entre entreprises implique naturellement des traitements de données à caractère personnel auxquels le RGPD s'applique, que ce soit les données des clients, du personnel ou des fournisseurs.

Les données à caractère personnel des clients présentent une valeur commerciale importante, tant pour le franchiseur que pour le franchisé, et sont d'ailleurs souvent collectées en masse. Ces données clients peuvent être des coordonnées de contacts, des données relatives aux paiements et cartes de paiement, des informations de géolocalisation, des tendances d'achats, etc. Toutes ces données, associées à des logiciels ou algorithmes de statistiques ou d'analyse, permettent notamment de mettre en place des programmes de fidélité personnalisables, de mieux cerner les intérêts des clients, de développer de nouveaux produits, etc.

Ces traitements de données présentent incontestablement des avantages mais ne sont pas sans risque au regard du RGPD.

Tout d'abord, les autorités de contrôle nationales peuvent sanctionner les infractions aux dispositions les plus importantes du RGPD par des amendes administratives dont les montants les plus élevés peuvent aller jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total. Outre une sanction pécuniaire significative, le manque de conformité aux règles en matière de la protection des données et de la vie privée peut ternir la réputation de l'entière du réseau de franchise. Entretemps, l'APD a pu infliger des amendes pouvant aller jusqu'à 30.000 euros (décision 77/2023), voire 100.000 euros (décision 56/2021).

Réseaux de franchise : le rôle de chaque partie au regard du RGPD

Afin de respecter le RGPD, il convient d'identifier d'abord le **responsable du traitement** : c'est en effet ce dernier qui doit respecter les dispositions du RGPD et démontrer la conformité au RGPD de ses activités (articles 5.2[1] et 24[2] du RGPD).[3] L'identification du responsable (ou des responsables conjoints) est donc primordiale dans un réseau de franchise, où les acteurs sont généralement nombreux. Nous remarquons de nombreuses confusions dans la pratique.

Comment identifier le responsable ou les responsables conjoints des traitements impliqués dans un réseau de franchise ? Selon le RGPD, le responsable du traitement est la personne (morale, physique ou toute autre entité) qui détermine les finalités et les moyens du traitement (article 4.7 du RGPD). Plusieurs personnes seront considérées comme des responsables conjoints quand les mêmes finalités et moyens ont été décidés conjointement et en même temps. **Le sous-traitant** est la partie qui traitera les données pour le compte et sur instructions du responsable du traitement (article 4.8 du RGPD).

Il n'existe donc pas de réponse toute prête et adéquate à tous les réseaux de franchise. En effet, la notion de responsable est une notion fonctionnelle et le RGPD impose d'identifier

le(s) responsable(s) sur base d'éléments factuels. Il n'est donc pas possible d'affirmer que tous les franchiseurs sont des responsables du traitement et tous les franchisés des sous-traitants (ou inversement).

Il n'est pas non **plus possible d'imposer le rôle de 'responsable du traitement' par voie contractuelle** quand les critères ne sont pas rencontrés factuellement, dans le chef de la personne désignée comme responsable du traitement. Les parties doivent donc procéder à une analyse au cas par cas.

La première question à se poser est la suivante : **qui a le pouvoir décisionnel** ou l'influence sur le traitement de données ? En d'autres termes, qui a initié le traitement de données ? Pourquoi le traitement est-il mis en place ?

Exemple 1 : Un réseau de distribution envisage de développer de nouveaux produits ou services. Pour ce faire, il souhaiterait disposer de statistiques sur la clientèle de son ou ses enseigne(s). Il fournit à tous ses franchisés un questionnaire à faire remplir par leurs clients, avec des instructions sur les informations à recueillir. Chaque franchisé effectue et transmet ensuite les résultats statistiques de cette étude à la tête de réseau (franchiseur). Les traitements de données, présents en l'espèce, sont la collecte des données et la réalisation d'évaluations statistiques avec ces données. Il se peut que les résultats statistiques soient des données pseudo-anonymisées ou anonymisées. Dès lors, bien qu'il n'ait reçu que des données statistiques et pas de données à caractère personnel à proprement parler, le franchiseur reste le responsable des traitements effectués pour réaliser les analyses. En effet, c'est le franchiseur qui a déterminé la finalité et les moyens de ces traitements et a instruit ses franchisés sur les traitements à réaliser. Le fait qu'il n'ait pas accès aux données traitées n'est pas déterminant.[4]

Le deuxième critère concerne **l'objet du pouvoir décisionnel** : Qui détermine les finalités et les moyens du traitement ? Les finalités et les moyens désignent respectivement le « **pourquoi** » et le « **comment** » du traitement.[5] Il existe aussi une hiérarchie entre les finalités et les moyens : le fait de déterminer la finalité entraîne d'office la qualification de responsable du traitement. Le sous-traitant dispose toutefois d'une certaine marge de manœuvre pour choisir comment implémenter un traitement de données.

Troisièmement, la **marge de manœuvre du sous-traitant n'est pas sans limite**. La qualification de 'responsable du traitement' peut également être appliquée quand une partie détermine les moyens essentiels des traitements de données. En général, la finalité, les catégories de données, la durée de conservation sont considérées comme des éléments essentiels des traitements. Quant aux moyens non essentiels, on parle du choix des logiciels, du matériel, des mesures de sécurité concrètes.

Exemple 2: Dans un réseau de franchise, le franchiseur met à la disposition de ses franchisés une base de données destinée à collecter et conserver les données des clients de l'enseigne. Cette base de données est hébergée sur les serveurs du franchiseur. Chaque franchisé y entre les données de ses clients, pour des finalités qui lui sont propres, et choisit, en toute indépendance, les durées de conservation, l'accès, la rectification et la suppression des données clients. Un franchisé ne peut accéder ou utiliser les données des autres franchisés. et le franchiseur ne peut accéder aux données entrées par les franchisés. Dans un tel cas de figure, le franchiseur est sous-traitant pour tous les franchisés car il a juste fourni des moyens non essentiels, c'est-à-dire un outil informatique dont les modalités sont laissées au choix des

franchisés, tandis que chaque franchisé est responsable de manière autonome de l'usage fait de la base de données. Le facteur déterminant dans ce cas est l'indépendance des franchisés dans le choix de la finalité, des types de données et des caractéristiques des traitements de données.

Une même partie peut accumuler deux rôles différents : Un franchisé peut traiter des données pour le compte du franchiseur, comme sous-traitant, et peut également, en dehors des instructions du franchiseur et pour des finalités qui lui sont propres, traiter des données en tant que responsable du traitement. Cependant, une partie ne peut accumuler des rôles différents pour le même ensemble de traitements.

Exemple 3 : Dans l'exemple 1, les franchisés sont des sous-traitants pour l'analyse des données. Cependant, ces données pourraient avoir été également collectées par les franchisés, auprès de leurs clients, en vue de l'élaboration de nouveaux services ou produits, et donc à des finalités différentes que l'analyse, telle la mise en place d'un système de **fidélité** fidélisation qui leur soit propre. Les franchisés seront dans ce cas responsables des traitements liés au système de fidélisation.

L'analyse des critères énoncés doit également être réalisée à la lumière d'autres facteurs, tels que le pouvoir de négociation de chaque partie, le degré d'indépendance des franchisés, le contenu des obligations contractuelles du contrat de franchise, etc.

En résumé, pour la protection des données de l'ensemble du réseau, le franchiseur prudent fera une analyse des flux de données qui circulent au sein de son réseau (tout en tenant compte de futurs projets) et, tenant compte de la complexité de l'attribution des responsabilités telle qu'illustrée ci-dessus, il aura intérêt à mettre en place les mesures nécessaires en vue de respecter le RGPD. A défaut, le réseau entier naviguera à l'aveugle et sera en risque au regard de l'application du RGPD.

Quelques points d'attention propres aux réseaux de franchise et conseils.

Les accords écrits entre responsables et sous-traitants

Dans le cadre d'une sous-traitance, le RGPD impose aussi bien au responsable du traitement qu'au sous-traitant, de rédiger un accord écrit relatif à ladite sous-traitance (article 28 du RGPD). Cet accord a pour but de définir les obligations et droits de chaque partie, mais aussi de contenir certaines informations énumérées à l'article 28 du RGPD.

Comme nous l'avons vu précédemment, certaines parties peuvent accumuler des rôles différents pour différents traitements. Cette obligation peut donc se révéler en réalité difficile à respecter et à mettre en place, au vu de la multiplicité des acteurs et des actions poursuivies dans un réseau de franchise.

Etant donné la relation contractuelle qui les lie, le franchiseur, quand il est responsable du traitement – et aussi par souci de réputation de son réseau-, devrait s'assurer que ses franchisés respectent la réglementation en vigueur. Pour ce faire, il est vivement recommandé d'insérer dans le contrat de franchise les obligations réciproques du franchisé et du franchiseur. En pratique, des lignes directrices sont incluses dans une annexe spécifique au

contrat de franchise, mais, trop souvent, les rôles de chacun, dans chaque cas de figure, ne sont pas suffisamment spécifiés. Cependant, en cas de violation du RGPD par un franchisé sous-traitant, l'existence-même d'une telle clause n'est pas suffisante pour déresponsabiliser le franchiseur : encore doit-il mettre en œuvre une telle clause, effectivement surveiller les actions de ses sous-traitants et prendre les mesures de sauvegarde nécessaires.

Une assistance du franchiseur conforme au RGPD

Un contrat de franchise prévoit généralement l'obligation dans le chef du franchiseur, d'assister ses franchisés par la fourniture d'outils techniques. Le franchiseur pourra offrir à ses franchisés des outils informatiques conformes au RGPD (respectant par exemple le principe de minimisation des données) mais aussi des outils de mise en conformité (documentation modèle sur la protection des données, audit, analyse d'impact des risques, procédure de réponse à des demandes de personnes concernées, registre des activités de traitement, etc.).

Le franchiseur pourrait également proposer à ses franchisés, à titre d'assistance, les services d'un Data Protection Officer (DPO). Les services d'un DPO interne (c'est-à-dire membre ou employé du franchiseur) offerts aux franchisés, pourraient toutefois s'avérer problématiques. Un DPO doit avoir la capacité d'agir en toute indépendance et donc, sans conflit d'intérêts avec les missions qu'il exerce auprès du franchiseur. De sorte que les franchisés puissent recevoir les conseils les plus adéquats et exempts de tout conflit d'intérêts, nous préconisons de recourir aux services d'un DPO externe.

Le respect des droits des personnes concernées

En vertu du RGPD, les personnes concernées disposent d'un certain nombre de droits qu'elles doivent exercer auprès du responsable du traitement (droit d'accès, droit de rectification, droit d'effacement, droit à la limitation, droit à la portabilité, droit d'opposition, droit de s'opposer au profilage – articles 15 à 22 du RGPD). Les sous-traitants ont eux l'obligation d'aider le responsable du traitement à respecter l'exercice de ces droits.

Dans un réseau de franchise, il est probable que des clients exercent leurs droits directement auprès des franchisés, généralement à l'insu du franchiseur. Il appartiendra alors au franchiseur de mettre en place des procédures avec ses franchisés, afin que les demandes introduites par des clients – relatives à des traitements dont il est responsable – lui soient transmises en temps utile.

Le responsable du traitement a également un devoir d'information à l'égard des personnes concernées (articles 13 et 14 du RGPD) et de faciliter l'exercice des droits des personnes concernées (article 12.2 du RGPD). Ces devoirs entraînent l'obligation d'informer clairement les personnes concernées sur l'identité du responsable du traitement, afin qu'elles puissent exercer leurs droits efficacement. Les franchisés étant généralement en contact direct avec la clientèle, le franchiseur pourrait alors leur imposer de transmettre à la clientèle les informations requises par le RGPD. Le franchiseur veillera d'ailleurs à communiquer à travers son ou ses sites internet et par tout moyen approprié.

L'importance d'un consentement valide ou pas ?

Il peut arriver que le franchiseur et ses franchisés se partagent la même base de données clients et que cette base de données soit utilisée à des fins de marketing direct par le franchiseur ou/et le franchisé.

Il est généralement accepté que le marketing direct se fonde soit sur le consentement des clients, soit sur l'intérêt légitime des entreprises. Bien qu'il n'existe pas de primauté entre les bases légales permises par le RGPD, beaucoup d'entreprises se fondent sur le consentement pour procéder à des campagnes publicitaires.^[6]

Dès lors, il convient pour toutes les parties d'un réseau de franchise d'être prudentes, quant à la justification des traitements de données de clients à des fins de marketing direct, plus particulièrement lorsqu'ils s'appuient sur le consentement de la clientèle. En effet, si un franchiseur/franchisé ne respecte pas les règles relatives au consentement pour collecter des données, le consentement ne pourra être considéré comme valable et le franchiseur/franchisé utilisant ces données, serait susceptible de violer le RGPD. Pour rappel, un consentement doit être éclairé, libre, spécifique et univoque et s'illustrer par un acte positif clair. Le responsable du traitement doit aussi être en mesure de démontrer la validité du consentement des personnes concernées.

Enfin, il est parfois plus efficace de recourir à une autre base légale que le consentement, vu qu'il serait fastidieux et absurde de tenter de recueillir le consentement de chaque .^[7]

Ainsi la conformité au RGPD peut être un exercice périlleux dans un réseau de franchise. Dès lors, il est important pour chaque réseau de franchise, d'avoir une bonne connaissance des flux de données au sein de son réseau, d'adapter régulièrement son dispositif contractuel avec ses partenaires et surtout, de mettre en place un système de mise en garde, de réception de plainte commun et de contrôle et d'évaluation des actions des franchisés. Les sanctions de l'APD et les risques d'atteinte à la réputation du réseau pousseront le franchiseur à garder la maîtrise du sujet et de poursuivre ses efforts de sensibilisation en la matière.

Benoit Simpelaere – Leonard Hawkes (DPO) – Tatiana De Schepper
FLINN LAW

^[1] Le responsable du traitement doit être en mesure de démontrer qu'il respecte les principes fondamentaux de la protection des données.

^[2] Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir et pouvoir démontrer que le traitement est effectué conformément au RGPD.

^[3] Concernant le rôle de responsable du traitement et de sous-traitant, voyez notamment le guide de la CEPD : Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées le 7 juillet 2021, disponible sur [edpb_guidelines_202007_controllerprocessor_final_fr.pdf \(europa.eu\)](https://edpb.europa.eu/edpb/files/2021/07/20210707_guidelines_202007_controllerprocessor_final_fr.pdf)

[4] CJUE, arrêt *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, § 38; CJUE, arrêt *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, § 69.

[5] Av. Gén. Bot dans l'arrêt *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, § 46.

[6] Concernant le marketing direct et les bases légales acceptées, voyez [Bases juridiques à vos traitements de marketing direct | Autorité de protection des données \(autoriteprotectiondonnees.be\)](#)

[7] Il convient de rappeler que l'envoi de courriers électroniques de prospection directe à des clients existants est permis sous certaines conditions, telles le fait que l'adresse électronique ait été obtenue directement auprès du client dans le cadre de la vente d'un produit ou d'un service et que la prospection porte sur un produit ou un service similaire. Il s'agit du « soft opt-in », une exception au principe du consentement préalable pour l'envoi de courriels de prospection. L'APD a expliqué les limites du soft opt-in dans sa décision 117/2022 du 26 juillet 2022, disponible en néerlandais.