Sous-traitants : la réutilisation de données confiées par un responsable de traitement

12 janvier 2022

Un sous-traitant ne peut réutiliser des données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial et que le responsable du traitement lui en a donné l'autorisation écrite.

Selon la définition donnée par le règlement général sur la protection des données (RGPD), un sous-traitant traite des données personnelles pour le compte du responsable du traitement. Dans ce cadre, il ne fait que suivre les instructions du responsable de traitement et ne peut pas, en principe, utiliser les données pour son propre compte. Il arrive toutefois qu'un sous-traitant souhaite réutiliser les données avec souvent pour objectif l'amélioration de ses services ou de ses produits ou la conception de nouveaux services et produits. **Une telle réutilisation n'est possible qu'à plusieurs conditions.**

Sous-traitants : une autorisation du client est nécessaire

Conformément au RGPD, le sous-traitant ne peut traiter (utiliser) les données personnelles auquel il a accès que sur instruction documentée du responsable du traitement. Le sous-traitant peut donc licitement traiter les données tant qu'il agit pour se conformer de la meilleure façon et la plus sûre possible aux instructions du responsable du traitement. En revanche, **il ne peut pas réutiliser ces données pour son propre compte, de sa propre initiative,** sauf si un texte national ou européen le lui impose.

Le sous-traitant qui réutiliserait les données de sa propre initiative **serait qualifié de responsable de ce traitement** et **passible de sanctions** pour ne pas avoir agi dans le respect des instructions du responsable du traitement initial.

Le **responsable du traitement peut toutefois, dans les conditions décrites ci-dessous, autoriser son sous-traitant à réutiliser pour son propre compte les données personnelles.** Le sous-traitant devient alors responsable de ce nouveau traitement.

Responsables de traitement : les conditions pour donner une autorisation

Procéder à un « test de compatibilité » avant d'accorder son autorisation

Une réutilisation des données par un sous-traitant pour une finalité propre constitue un traitement dit « ultérieur », c'est-à-dire un traitement qui suit l'opération de collecte et qui a une finalité différente de celle justifiant la collecte initiale.

Le responsable du fichier doit **déterminer si ce traitement ultérieur est compatible avec la finalité pour laquelle les données ont été initialement collectées**, lorsque le traitement ne s'appuie pas sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre.

Pour cela, il doit notamment tenir compte :

- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données personnelles ont été collectées et les finalités du traitement ultérieur envisagé ;
- du contexte dans lequel les données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données personnelles, en particulier si le traitement porte sur des données sensibles ou des données personnelles relatives à des condamnations pénales et à des infractions;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Exemple : un sous-traitant souhaite réutiliser des données pour une finalité d'amélioration de ses prestations de *cloud computing*. Cette réutilisation pourrait être considérée compatible avec le traitement initial, sous réserve de garanties appropriées telle que l'anonymisation des données si ces données identifiantes ne sont pas nécessaires. En revanche, leur réutilisation pour une finalité de prospection commerciale satisferait difficilement le « test de compatibilité ».

Si le test n'est pas satisfait, le responsable du traitement doit refuser de donner son autorisation à la réutilisation des données. Si le test est satisfait, le responsable du traitement est libre de donner ou non son accord.

Pas d'autorisation préalable et générale

Ce « test de compatibilité » doit être réalisé pour un traitement déterminé, en tenant compte des finalités et des caractéristiques de chaque traitement pour lequel le sous-traitant souhaite réutiliser les données.

Cela signifie qu'une autorisation préalable et générale de réutilisation des données n'est pas légale.

L'autorisation doit être écrite

L'autorisation du responsable du traitement initial doit être établie par écrit, y compris en format électronique.

Le RGPD impose, en effet, un contrat ou tout autre acte juridique écrit pour encadrer le traitement mis en œuvre par un sous-traitant.

Le partage des obligations du RGPD

Le responsable du traitement initial doit informer les personnes concernées

Il revient, en principe, au responsable du traitement initial d'informer les personnes concernées de la transmission des données à un nouveau responsable de traitement, pour une nouvelle finalité. Il doit notamment indiquer s'il est possible de s'y opposer. En pratique, il est recommandé que le responsable de traitement initial procède, si c'est possible, à l'ensemble de l'information sur le traitement.

Si le sous-traitant détient déjà les données de contact des personnes concernées, le responsable de traitement initial peut déléguer cette action au sous-traitant pour le traitement qu'il souhaite réaliser.

Le responsable du traitement ultérieur (ex-sous-traitant) doit s'assurer de la conformité du traitement

En réutilisant des données, le sous-traitant du responsable du traitement initial devient responsable du traitement ultérieur : **il devient donc responsable de la conformité de son traitement à l'ensemble des exigences du RGPD**. À défaut, il peut être sanctionné par la CNIL en tant que responsable de ce traitement.

Il doit notamment traiter les données en respectant la règlementation. Cette exigence n'est pas satisfaite s'il traite des données pour une finalité incompatible avec la finalité initiale ou sans l'autorisation écrite et valable du responsable du traitement initial.

En tant que responsable du traitement ultérieur, il doit en outre s'assurer que celui-ci réponde à une finalité bien définie et repose sur une base légale adaptée à cette finalité.

Par ailleurs, il doit notamment :

- fournir aux personnes concernées, sauf exceptions applicables, les informations sur cette collecte indirecte qui n'auraient pas déjà été délivrées par le responsable du traitement initial;
- définir une durée de conservation adéquate des données ;
- ne collecter que les données nécessaires pour répondre à la finalité fixée au départ (minimisation) ;
- permettre l'exercice des différents droits par les personnes concernées ; ou encore
- mettre en place toutes les mesures de sécurité nécessaires.

Texte reference

Pour approfondir

> Travailler avec un sous-traitant
Texte reference

Les textes de référence

> Article 6.4 du RGPD (vérification de la compatibilité des finalités en cas de réutilisation de données)
> Article 28 du RGPD (sous-traitants)
> Article 29 du RGPD (responsabilité du sous-traitant sous l'autorité du responsable de traitement)
> Lignes directrices 07/2020 du Comité européen de la protection des données (CEPD) sur les notions de responsable de traitement et de sous-traitant au sens du RGPD (en anglais) – edpb.europa.eu