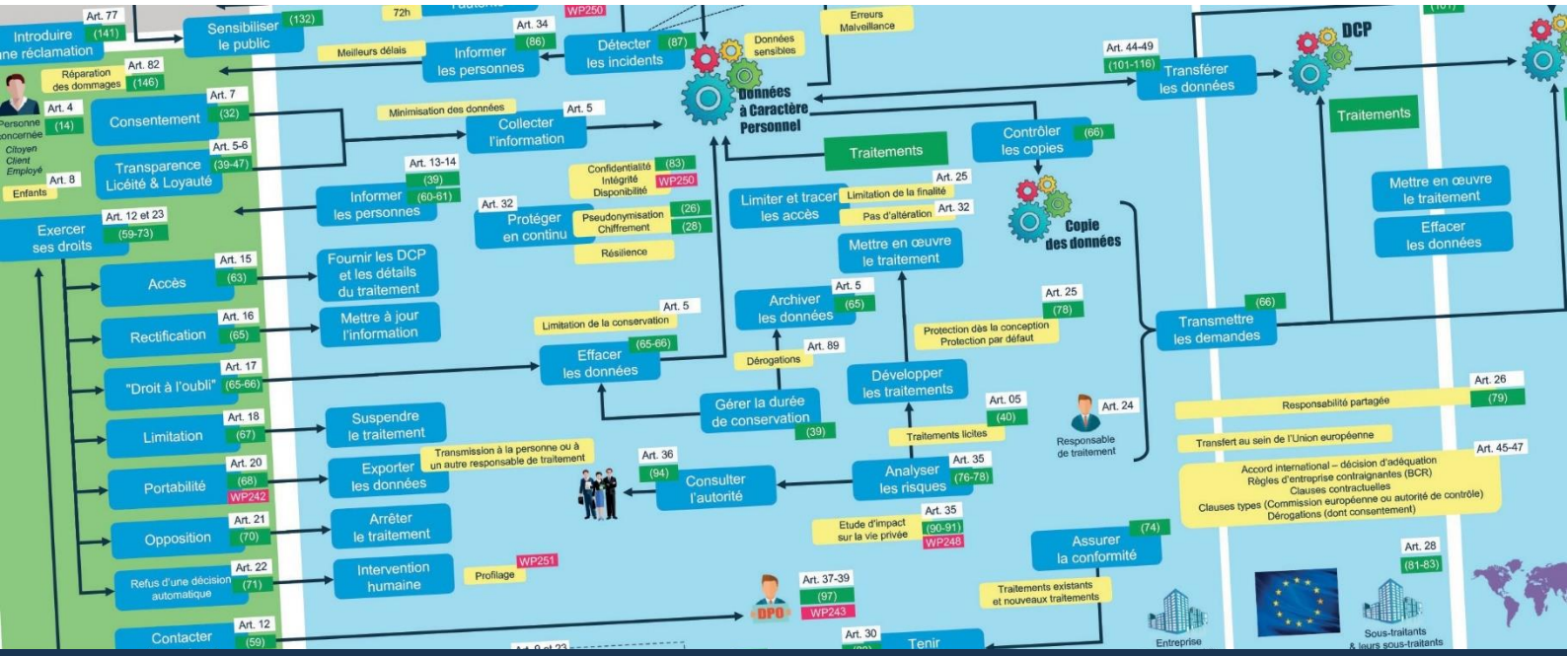
LES FICHES PRATIQUES du CLUSIF - RGPD



RESPONSABILITÉ DES SOUS-TRAITANTS

1. DÉFINITIONS

Le sous-traitant est défini dans le règlement comme « [une] *personne physique ou morale*, [une] *autorité publique*, [un] *service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* » (*RGPD, Art. 4, 8*).

La distinction entre la qualification de « *responsable du traitement* » et de « *sous-traitant* » porte sur la répartition de la responsabilité de chacun.

Le prestataire qui traite des données personnelles pour le compte, sur instruction et sous l'autorité du responsable de traitement est un sous-traitant au sens juridique du terme. Le guide élaboré par la CNIL relatif à la sous-traitance propose une analyse au cas par cas pour déterminer le statut du prestataire vis-à-vis du règlement en tenant compte des éléments suivants :

- Le niveau d'instruction donné par le client au prestataire : quelle est l'autonomie du prestataire dans la réalisation de sa prestation ?
- Le degré de contrôle de l'exécution de la prestation : quel est le degré de « surveillance » du client sur la prestation ?
- La valeur ajoutée fournie par le prestataire : le prestataire dispose-t-il d'une expertise approfondie dans le domaine ?
- Le degré de transparence sur le recours à un prestataire : l'identité du prestataire est-elle connue des personnes concernées qui utilisent les services du client ?

Selon les cas, le prestataire pourra être qualifié de sous-traitant, ou de responsable conjoint de traitement au regard du RGPD. En effet, lorsque deux responsables de traitement ou plus, déterminent conjointement les finalités (pourquoi) et les moyens (comment) du traitement, ils sont responsables conjoints du traitement (*RGPD, Art. 26*).

Exemple : une collectivité met en œuvre un traitement pour gérer le covoiturage, et met ce traitement à la disposition d'une autre collectivité. Dans ce cas, les deux collectivités sont responsables conjoints.

2. OBLIGATIONS DES SOUS-TRAITANTS

Si les obligations de la loi Informatique et Libertés (avant le RGPD) ne s'imposaient qu'au responsable de traitement, le règlement consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles. En cas de manquement aux exigences du RGPD, les responsables de traitement et leurs sous-traitants seront solidairement responsables vis-à-vis de la personne concernée (*RGPD, Art. 28*).

Le règlement amplifie ainsi les devoirs antérieurs des responsables de traitement et des sous-traitants tout en organisant un régime de sous-traitance en matière de protection des données personnelles, distinct des devoirs de sécurité.

Comme auparavant, le responsable du traitement ne peut choisir que des sous-traitants présentant des garanties suffisantes pour la prise de mesures techniques et opérationnelles appropriées afin de se conformer aux prescriptions règlementaires et assurer la protection des droits de la personne concernée (*RGPD, Art 28*). Cela implique :

- Une obligation de transparence et de traçabilité (notamment au travers d'un contrat) ;
- La prise en compte des principes de protection des données dès la conception et de protection des données par défaut (cf. fiche dédiée) ;
- Une obligation de garantir la sécurité des données traitées ;
- Une obligation d'assistance, d'alerte et de conseil.

Le responsable de traitement devra ainsi veiller à ce que son sous-traitant respecte le règlement ainsi que les obligations spécifiques qui s'imposeront à eux. Le sous-traitant doit en particulier aider le responsable de traitement dans sa démarche permanente de mise en conformité de ses traitements. Ces obligations concernent tous les organismes qui traitent des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation. Sont notamment concernés :

- Les prestataires de services informatiques (hébergement, maintenance, …) ;
- Les intégrateurs de logiciels ;
- Les sociétés de sécurité informatique ;
- Les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données ;
- Les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients.

Les hébergeurs, notamment SaaS, ainsi que les entreprises qui gravitent autour du numérique (Web marketing, e-commerçants, commerces autour des objets connectés…) sont des sous-traitants au sens du règlement. À l'inverse, les éditeurs de logiciels ou les fabricants de matériels ne sont pas des sous-traitants au sens du RGPD, et ne sont donc pas concernés par ces dispositions.

Les obligations des sous-traitants doivent être définies en fonction de trois niveaux de risque de la manière suivante :

- Les prestataires sans accès direct aux données à caractère personnel ;
- Les prestataires ayant un accès important à certaines données à caractère personnel ;
- Les prestataires ayant un accès total aux données à caractère personnel.

3. ORGANISATION CONTRACTUELLE

Le principe reste encore celui d'une organisation contractuelle spécifique entre le responsable du traitement et le sous-traitant. Le contenu du contrat écrit est élargi.

Outre des informations sur le traitement lui-même (finalité, objet et durée du traitement, etc.), conformément à l'article 28 du RGPD, le contrat doit prévoir l'engagement du sous-traitant à respecter toute une série de devoirs à l'égard du responsable, notamment :

- Ne traiter les données que sur instructions documentées du responsable de traitement – notamment les transferts de données vers des pays tiers ;
- Intégrer des clauses de sécurité (confidentialité, intégrité) ;

- Respecter les conditions de recrutement d'un autre sous-traitant secondaire ;
- Prévoir des clauses pour l'*accountability* et le soutien au responsable de traitement (réalisation des analyses d'impact, registre de traitement, exercice des droits des personnes) ;
- Aider le responsable à garantir le respect de ses propres obligations de sécurité (clauses pour la notification des violations de données) ;
- Prévoir des clauses concernant la suppression ou la restitution des données en fin de contrat après l'exécution du service ;
- Mettre à la disposition du responsable toutes les informations nécessaires pour démontrer le respect de l'article 28 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.

La revue des contrats est donc primordiale pour se mettre en adéquation avec le règlement. La précision et l'élargissement des mentions contractuelles, étendues aux liens de sous-traitance secondaire, imposent aux responsables de revoir toutes leurs relations avec leurs sous-traitants et donc de modifier profondément les contrats antérieurs. Souvent, en pratique, des mentions assez générales étaient contenues au mieux dans une seule clause de style insérée dans le contrat de prestation de service.

Le sous-traitant – souvent un prestataire technique – devra impérativement accorder plus d'importance à la protection des données et à ses obligations qui dépassent la simple prise de mesures de sécurité.

Des exemples de clauses sont disponibles dans le guide de la CNIL :
https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

Parmi les nouvelles obligations du sous-traitant, la désignation d'un DPO, si nécessaire, la tenue d'un registre des activités de traitement, la notification des violations de données, la gestion des demandes d'exercice des droits des personnes concernées, etc. sont autant de sujets qui doivent faire l'objet d'une attention particulière de la part du responsable de traitement.

4. SOUS-TRAITANCE SECONDAIRE

Le règlement organise la question de la sous-traitance confiée à des tiers – sous-traitants secondaires – par le sous-traitant direct du responsable de traitement. Ainsi, la possibilité laissée au sous-traitant de sous-traiter lui-même devra faire l'objet d'un accord écrit préalable (spécifique ou général) du responsable de traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant direct doit informer le responsable de traitement, préalablement à tout changement de sous-traitant secondaire en vue de donner au responsable de traitement la possibilité d'émettre des objections.

Ce contrat de sous-traitance secondaire devra obéir lui-même aux règles de contenu applicables au contrat conclu entre le responsable de traitement et le sous-traitant principal. Le sous-traitant direct est responsable devant le responsable de traitement de la mauvaise exécution des obligations contractuelles de ses propres sous-traitants.

L'adhésion du sous-traitant à un code de conduite visé à l'article 40 du RGPD ou à un mécanisme de certification approuvé visé à l'article 42 peut être utilisé pour démontrer l'existence de garanties suffisantes par le sous-traitant.

Le règlement prévoit expressément la possibilité d'utiliser des clauses contractuelles types fournies par diverses sources comme fondement du contrat particulier entre le responsable de traitement et le sous-traitant (incluses dans une procédure de certification, de la Commission ou d'autorités de contrôle).

Sources :
https://www.gdpr-expert.eu/article.html?id=28#ouvaton
https://www.lexgo.lu/fr/articles/ip-it-telecom/droit-de-l-informatique/outsourcing-contracts-under-the-general-data-protection-regulation-more-revolution-than-evolution,108155.html
https://www.avocats-mathias.com/conseil-de-la-semaine/sous-traitant-donnees-personnelles