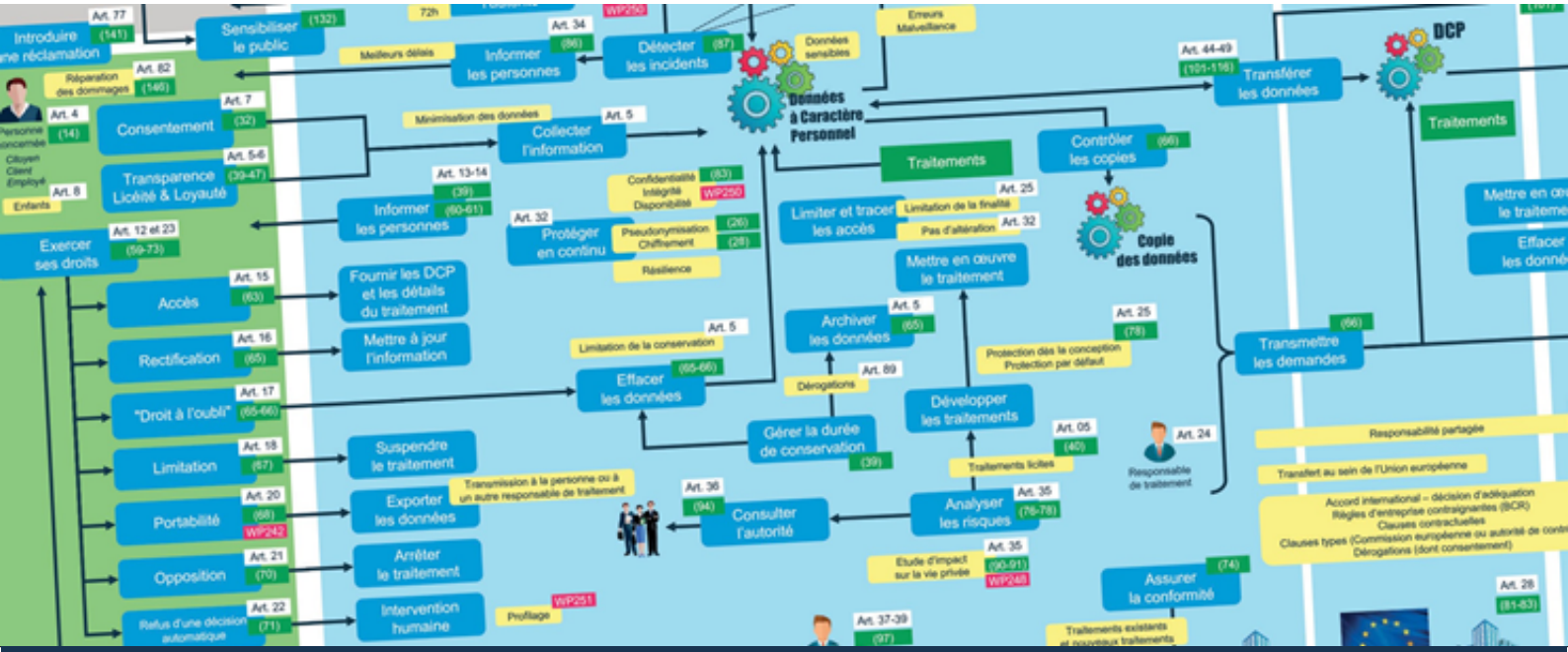
CLUSIF

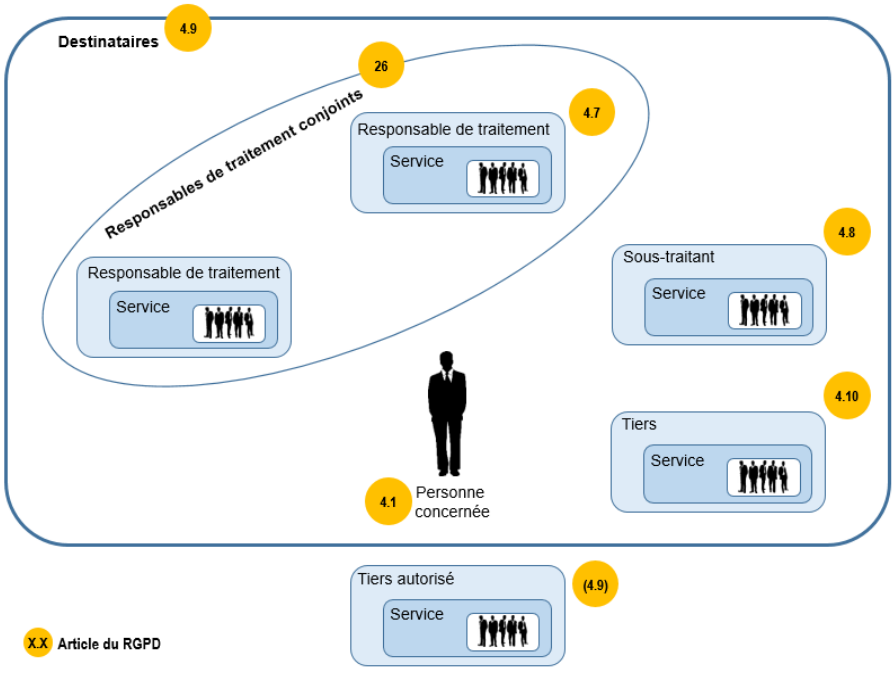
LES GUIDES PRATIQUES du CLUSIF - RGPD



LA RESPONSABILITÉ DES ACTEURS

Le règlement européen pose un principe de responsabilisation de l'ensemble des organismes impliqués dans les traitements de données ciblant des résidents européens, que ces organismes soient ou non établis au sein de l'Union européenne (UE) et qu'ils agissent en qualité de responsable de traitement ou de sous-traitant.

Sont précisées dans la présente fiche les responsabilités des acteurs suivants : responsable de traitement (RT), sous-traitant (ST), délégué à la protection des données (DPO), destinataires des données et tiers autorisés, représentants des RT ou ST hors UE.



RESPONSABLES DE TRAITEMENTS ET SOUS-TRAITANTS

Le règlement rééquilibre les situations juridiques des responsables de traitements, des responsables conjoints et des sous-traitants qui voient leurs obligations précisées et leur responsabilité susceptible d'être conjointement engagée.

1. Responsabilité du responsable de traitement

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse prévue par les dispositions législatives ou réglementaires relatives à ce traitement, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (RGPD, Art. 4.7).

Le responsable de traitement est l'un des principaux acteurs impliqués dans le cadre du règlement sur les données à caractère personnel. Pour l'identifier, il convient de déterminer sa capacité juridique et organisationnelle, ainsi que son autonomie dans la définition des finalités et des moyens du traitement.

En pratique, il s'agit de la personne morale incarnée par son représentant légal. Il met en œuvre le traitement dans son intérêt, en son propre nom et pour son propre compte. Les employés traitant les données à caractère personnel au sein de l'organisation agissent pour exécuter les missions confiées par le responsable du traitement.

Il existe une exception selon laquelle le responsable de traitement peut être désigné par un texte législatif ou réglementaire. Dans ce cas l'interprétation est simplifiée, puisqu'il est directement identifié par le texte (à titre d'exemple, la Fondation du patrimoine, définie par l'article L. 143-1 du code du patrimoine, est l'organisme responsable de traitement pour la sauvegarde et la conservation du patrimoine français).

❖ Responsabilité conjointe des responsables de traitement

Le principe de responsabilité conjointe de traitement des données à caractère personnel avait été pris en compte dans la directive 95/46/CE (article 2.d). Elle était caractérisée lorsque plusieurs responsables de traitements concouraient à la définition des finalités et des moyens du traitement. Lors de la transposition de la directive en 2004, le législateur français n'avait cependant pas consacré ce principe dans la loi Informatique et Libertés. Le responsable de traitement n'est pas toujours unique. Il peut exercer ses missions conjointement avec un ou plusieurs autres responsables de traitement.Il y a responsabilité conjointe du traitementt « comment » les données à caractère personnel devraient être traitées (RGPD, Art. 26).

La situation de responsabilité conjointe implique de définir les obligations respectives des responsables de traitement. La responsabilité conjointe implique l'établissement d'un accord (sauf si elles résultent du droit de l'Union européenne ou d'un État membre) afin de définir, de manière transparente, les rôles et obligations de chacun, ainsi que le respect des droits des personnes et l'obligation d'information. Le règlement prévoit également des obligations propres à chaque responsable de traitement, et notamment :

- La tenue d'un registre des traitements ;
- La coopération avec l'autorité de contrôle ;
- La mise en place de mesures techniques et organisationnelles pour protéger les données à caractère personnel ;
- Le respect des droits fondamentaux des personnes concernées ;
- La notification des violations de données...

Par ailleurs, en cas de recours à un sous-traitant, celui des responsables de traitement partie au contrat devrait s'assurer des garanties présentées par le prestataire et de la satisfaction du contrat avec les exigences du règlement européen.

A noter que :

- Le RGPD prévoit que « les grandes lignes » de l'accord devront être mises à la disposition de la personne concernée par le traitement, sans préciser pour autant les modalités de cette mise à disposition (RGPD, Art. 26) ;
- Les personnes concernées pourront exercer leurs droits à l'égard et à l'encontre de chacun des responsables, peu importe les termes de l'accord.

Pour aller plus loin, voir les fiches :

FAQ Les notions de données à caractère personnel, de traitement et de responsable de traitement

FAQ Les obligations du responsable de traitement

2. Responsabilité du sous-traitant

❖ Rappel : Qu'est-ce qu'un sous-traitant ?

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 à caractère personnel 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).

❖ Quelles responsabilités pour le sous-traitant ?

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 à caractère personnel. En cas de manquement aux exigences du règlement, 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 à caractère personnel, distinct des devoirs de sécurité.

Lorsqu'un organisme intervient en tant que sous-traitant dans la mise en œuvre d'un traitement de données à caractère personnel, il doit offrir à son client, responsable de traitement « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (RGPD, Art. 28).

Les sous-traitants ont notamment une obligation de conseil auprès des clients pour le compte desquels ils traitent des données. Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (étude d'impact sur la vie privée, notification de violation de données, sécurité,

a. Obligation de transparence et de traçabilité :

 Existence d'un contrat ou d'un autre acte juridique précisant les obligations de chacune des parties et reprenant les dispositions de l'article 2 du règlement ;

 Recensement par écrit des instructions documentées du responsable de traitement ;

 Autorisation écrite du responsable de traitement en cas de recours à une sous-traitance secondaire ;

 Mise à disposition du responsable de traitement de toutes les informations de nature à démontrer le respect des obligations du sous-traitant et afin de permettre la réalisation d'audits ;

 Tenue d'un registre qui recense les clients du sous-traitant et décrit les traitements réalisés pour le compte des responsables de traitements.

b. Obligations en matière de sécurité, de confidentialité et de documentation :

 Les sous-traitants doivent prendre en compte la protection des données dès la conception du service ou du produit et par défaut, et mettre en place des mesures permettant de garantir une protection optimale des données ;

 Les employés du sous-traitant qui traitent les données du responsable de traitement doivent être soumis à une obligation de confidentialité ;

 Notification au responsable de traitement de toute violation de ses données ;

 Mesures garantissant un niveau de sécurité adapté aux risques ;

 Aux termes de la prestation et en accord avec les instructions du responsable de traitement, obligation de supprimer les données, de les anonymiser ou de les restituer au responsable de traitement.

c. Obligations d'assistance et de conseil.

Dans certains cas, ils devront également désigner un délégué à la protection des données dans les mêmes conditions qu'un responsable de traitement.

3. Quels risques en cas de non-respect des obligations ?

D'une manière générale, toute personne ayant subi un dommage (au sens large) matériel ou moral du fait d'une violation du règlement européen peut obtenir la réparation intégrale de son préjudice de la part du responsable de traitement ou du sous-traitant (RGPD, Art. 82).

Tout responsable de traitement ayant participé au traitement est ainsi considéré comme responsable du dommage causé par le traitement qui constitue une violation de l'une des dispositions du règlement. Le sous-traitant n'est quant à lui responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le règlement qui lui incombent spécifiquement ou s'il agit en dehors des instructions licites du responsable de traitement ou contrairement à celles-ci.

Il peut cependant être exonéré de toute responsabilité s'il apporte la preuve que le dommage ne lui est pas imputable.

Le responsable de traitement ou le sous-traitant peut donc être tenu pour responsable du dommage causé et le cas échéant faire l'objet de sanctions administratives (selon la catégorie de l'infraction, jusqu'à 10 ou 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % ou 4 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu).

S'agissant du sous-traitant, des sanctions peuvent s'appliquer (RGPD, Art. 83) :

- Si le ST agit en dehors des instructions licites du RT et contrairement à ces instructions ;
- Si le ST n'aide pas le RT à respecter ses obligations ;
- Si le ST ne met pas à disposition du RT les informations permettant de démontrer le respect de ses obligations ou pour permettre la réalisation d'audits ;
- En cas de non-respect de l'obligation de conseil (exemple : le ST n'informe pas le RT qu'une instruction constituerait une violation du règlement) ;
- En cas de recours à une sous-traitance secondaire sans autorisation écrite préalable du responsable de traitement ou ne présentant pas de garanties suffisantes ;
- En l'absence de désignation d'un délégué à la protection des données lorsque cela est obligatoire ;
- En l'absence de tenue d'un registre des activités de traitement.

Pour aller plus loin, voir :

FAQ, fiche sur La responsabilité des sous-traitants.

Le guide du sous-traitant de la CNIL

LE DELEGUE A LA PROTECTION DES DONNÉES

1. Quelle responsabilité pour le DPO ?

Il n'existe pas de responsabilité juridique spécifique du délégué à la protection des données. Les lignes directrices du CEPD précisent que le délégué n'est pas responsable en cas de non-respect du règlement. Le CEPD établit clairement que c'est le responsable du traitement ou le sous-traitant qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (RGPD, Art. 24.1). Le rôle du délégué à la protection des données est d'informer, de contrôler et de conseiller. Il appartient au responsable de traitement de décider l'application des avis ou recommandations du délégué.

Seul le responsable du traitement ou le sous-traitant devra ainsi répondre des manquements relatifs à la protection des données constatés par l'autorité de contrôle. Le respect de la protection des données relève donc de la responsabilité du RT ou du ST.

Il n'est pas possible de transférer au délégué, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant. Cela reviendrait à conférer au délégué, qu'il soit interne ou externe, un pouvoir décisionnel sur la finalité et les moyens du traitement, ce qui serait constitutif d'un conflit d'intérêts contraire à l'article 38.6 du RGPD.

En outre, les vérifications réalisées par le DPO dans le cadre de l'exercice de sa mission de contrôle du respect du règlement par l'entité qui l'a désigné et, plus généralement, de toute disposition relative à la protection des données - ce qui inclut les lignes directrices, guides, politiques et/ou procédures élaborés en interne - n'auront pas davantage pour effet de lui conférer la responsabilité des manquements qu'il pourrait constater.

2. Dans quelles hypothèses le DPO pourrait-il voir sa responsabilité pénale engagée ?

Comme n'importe quel collaborateur de l'organisme ou prestataire de service, le délégué à la protection des données peut voir sa responsabilité pénale engagée :

- S'il enfreint de façon intentionnelle les dispositions pénales contenues dans un texte législatif ou réglementaire (et pas uniquement celles contenues dans la loi Informatique et Libertés) ;

- S'il aide le responsable du traitement ou le sous-traitant à enfreindre lesdites dispositions pénales.

3. Quelle protection pour le DPO ?

Le délégué à la protection des données interne à l'organisme doit agir d'une manière indépendante et bénéficier d'une protection suffisante dans l'exercice de ses missions. Le règlement prévoit que le délégué ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions.

Les sanctions ne sont pas possibles si elles sont imposées en raison de l'exercice par le délégué de sa fonction. À titre d'exemple, si un délégué estime qu'un traitement est susceptible d'engendrer un risque élevé et conseille au responsable de traitement de procéder à une analyse d'impact, et si le responsable de traitement n'est pas d'accord avec l'analyse du délégué, ce dernier ne peut être relevé de sa fonction pour avoir formulé ce conseil.

À noter toutefois que le délégué n'est pas un salarié protégé au sens du Code du travail français. Dès lors, il pourrait être licencié légitimement, comme tout autre collaborateur, pour une faute professionnelle.

Comme tout autre collaborateur, à des fins de traçabilité, le délégué à la protection des données doit, et a tout intérêt à, documenter son activité.

Pour aller plus loin :

Voir FAQ, fiche sur Le Délégué à la protection des données.

LES DESTINATAIRES ET LES TIERS AUTORISÉS

Le règlement et la loi Informatique et Libertés imposent qu'un responsable de traitement, au regard de la nature des données et des risques présentés par chaque traitement de données à caractère personnel, prenne toutes les précautions utiles pour préserver la sécurité des données à caractère personnel dont il est responsable, et notamment qu'il empêche les tiers non autorisés d'y accéder.

Il doit dès lors prendre un certain nombre de précautions lorsqu'il envisage de communiquer ou de rendre accessibles ces données.

1. Les destinataires des données à caractère personnel

Le règlement définit le destinataire des données comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers » (RGPD, Art. 4.9) .

Le tiers est quant à lui défini comme « une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable de traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel » (RGPD, Art. 4.10).

Il exclut de cette définition les autorités publiques qui sont susceptibles de recevoir communication de ces données dans le cadre d'une mission d'enquête particulière conformément au droit de l'UE ou au droit d'un État membre.

En substance, le destinataire des données est donc la personne ou l'organisme auquel le responsable de traitement transmet les données à caractère personnel de sa propre initiative. Ces destinataires des données se distinguent des tiers autorisés, personnes ou organismes pouvant obtenir la communication de données en vertu d'une disposition législative ou réglementaire (cf. infra). Au vu de cette définition, voici les catégories des destinataires qui peuvent être envisagées :

- Le sous-traitant ➔ cf. supra
- Les collaborateurs internes de l'organisme ➔ Ils sont responsables des données traitées dans le cadre de leurs missions et doivent respecter les obligations imposées par le responsable de traitement ;
- Les destinataires externes ;
- Les responsables conjoints de traitement ➔ cf. supra
- Les responsables de traitement externes ➔ cf. supra
- Les personnes concernées (dans le cadre de l'exercice de ses droits ou parce qu'elles peuvent avoir accès aux données) ;
- Les tiers.

2. Les tiers autorisés

Le règlement et la loi Informatique et Libertés permettent à certaines administrations ou autorités publiques de se faire communiquer, sous certaines conditions et dans le cadre de leurs missions particulières ou de l'exercice d'un droit de communication des données à caractère personnel issues de fichiers ou traitements détenus par des organismes, publics ou privés. Ces tiers sont exclus de la définition de destinataire des données prévue par le règlement (RGPD, Art. 4.9) et sont dénommés « tiers autorisés » par la CNIL.

Une délibération de la CNIL datée du 2 février 1982, avant l'entrée en vigueur du RGPD, insistait sur les éléments suivants :

- La demande doit préciser le texte législatif ou réglementaire fondant ce droit de communication ainsi que les catégories d'informations sollicitées
- La communication ne peut être effectuée que :
    - Sur demande ponctuelle, écrite et motivée ;
    - Visant des personnes nommément désignées, identifiées directement ou indirectement ;
- Cette communication ne peut en outre porter sur

1 A noter que la loi Informatique et Libertés, dans sa rédaction antérieure à l'ordonnance 2018-1125 du 12 décembre 2018, considérait que le destinataire était nécessairement une personne extérieure à l'organisme responsable de traitement. Elle excluait donc de la définition des destinataires de données la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, étaient chargées de traiter les données (LIL, Art. 3).

2 Délibération de la CNIL 82-02 du 2 février 1982 portant adoption d'un conseil relatif à la communication à des tiers des renseignements d'ordre inatif figurant dans les fichiers d'EDF et de GDF.

l'intégralité d'un traitement, d'un sous-ensemble de traitements ou qu'elle aboutisse à l'organisation d'interconnexions.

Lorsqu'il est confronté à une demande de communication venant d'un tiers autorisé s'appuyant sur un texte, le responsable de traitement doit donc s'assurer que la disposition avancée est en vigueur et qu'elle prévoit effectivement un droit de communication au bénéfice du demandeur. Il doit par la suite veiller à ne transmettre que les données prévues par le texte ou, en cas d'imprécision de ce dernier, les seules données qui lui apparaissent strictement nécessaires pour atteindre l'objectif recherché. La communication des données devra être réalisée selon des modalités permettant de s'assurer de leur sécurité, en adaptant la mesure retenue à la nature des données et aux risques en présence. À noter qu'il n'est pas obligatoire d'informer les personnes concernées des transmissions de données au profit de tiers autorisés.

En application de dispositions législatives ou réglementaires, sont ainsi notamment considérés comme des tiers autorisés à obtenir ponctuellement des données à caractère personnel les organismes suivants (liste non exhaustive) :

Administration des impôts, des douanes et de l'économie	- Direction générale des finances publiques, Administration fiscale, - Direction générale des douanes, - Fonctionnaires des douanes, - INSEE…
Administration de la justice, de la police et de la gendarmerie	- Magistrats (à l'occasion de procédures judiciaires), - Officiers de police judiciaire de la police et de la gendarmerie (dans le cadre d'enquêtes préliminaires, de flagrance ou sur commission rogatoire), - Huissiers de justice chargés de l'exécution, techniciens experts judiciairement désignés (pour l'exécution de mesures d'instruction), - Auditeurs de la Cour des comptes…
Administrations de l'action sociale et autorités sanitaires	- Organismes débiteurs de prestations familiales (caisses d'allocations familiales dans le cadre du contrôle de l'exactitude des déclarations des allocataires, des demandeurs ou des bailleurs, en vue du recouvrement des créances alimentaires impayées…), - Agents des organismes de sécurité sociale, les contrôleurs des organismes de recouvrement des cotisations (URSSAF , CGSS …), - L'ANSES dans le cadre de sa mission d'évaluation des risques et de préservation de la santé publique, - Santé publique France dans le cadre de ses missions de surveillance de l'état de santé de la population, de veille sanitaire, d'alerte et de gestion des situations de crise, -Les inspecteurs des affaires sociales, de la santé publique, de l'action sanitaire et sociale, des agences régionales de santé, l'ANSM dans le cadre du contrôle du respect des dispositions législatives et réglementaires relatives à la santé publique…
Administrations du travail, de l'emploi et de la formation professionnelle	- Inspecteurs et contrôleurs du travail et de la formation professionnelle continue…

3 URSSAF : Unions de Recouvrement des cotisations de Sécurité Sociale et d'Allocations Familiales
4 CGSS : Caisses générales de sécurité sociale
5 ANSES : Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail
6 ANSM : Agence nationale de sécurité du médicament et des produits de santé

Autorités administratives indépendantes	- Autorité des marchés financiers, CNIL, conseil supérieur de l'audiovisuel, médiateur de la République, autorité de la concurrence… (dans le cadre de leurs missions de contrôle de la régularité des opérations effectuées)…
Autres tiers autorisés	- Commissaires aux comptes (contrôle de la régularité et de la sincérité des comptes annuels), - Commissions d'enquête parlementaires (dans le cadre des investigations qu'elles mènent sur des faits déterminés ou sur la gestion des services publics ou des entreprises nationales)…

LE REPRÉSENTANT DU RT OU DU ST

Le règlement définit le représentant comme étant « une personne physique ou morale établie dans l'UE, désignée par le RT ou le ST par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement » (RGPD, Art. 4.17).

Le rôle du représentant du responsable du traitement ou du sous-traitant établi hors de l'Union européenne est précisé à l'article 27 et au considérant 80 du règlement.

Le représentant agit dans l'hypothèse où le responsable de traitement ou le sous-traitant qui n'est pas établi dans l'Union européenne traite des données à caractère personnel de personnes concernées qui se trouvent dans l'UE dans le cadre :

1. D'offres de biens ou de services à ces personnes, qu'un paiement leur soit demandé ou non ;

2. Du suivi de leur comportement dans la mesure où celui-ci a lieu au sein de l'UE.

Dans ces conditions, le responsable de traitement ou le sous-traitant doit désigner un représentant sauf (RGPD, Art. 27 et cons. 80) (conditions cumulatives) :

 Si le traitement est occasionnel ;

 S'il n'implique pas un traitement à grande échelle de catégories particulières de données à caractère personnel (données dites « sensibles ») ;

 S'il n'implique pas un traitement de données relatives à des condamnations pénales et à des infractions ;

 S'il est « peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement ou si le responsable detraitement est une autorité publique ou un organisme public ».

Le représentant doit être établi dans l'État où se trouvent les personnes physiques concernées dont le responsable de traitement ou le sous-traitant offre des services ou dont le comportement est suivi.

Un contrat lie le représentant au RT ou au ST.

Le règlement européen précise les obligations du représentant :

 Devoir d'information : s'identifier dans le registre des traitements ainsi qu'au moment d'informer les personnes, accomplir l'obligation d'information des personnes concernées ;

 Point de contact : être le contact du responsable de traitement pour les personnes concernées et pour les autorités de contrôle concernant toute question relative à un traitement aux fins d'assurer le respect des dispositions du règlement ;

 Registre des traitements : tenir le(s) registre(s) du responsable de traitements et/ou sous-traitant et le(s) mettre à disposition de l'autorité de contrôle ;

 Coopération : coopérer avec l'autorité de contrôle et lui communiquer toute information nécessaire.

Le considérant 80 du RGPD indique que le représentant doit agir pour le compte du responsable du traitement ou du sous-traitant. La désignation de ce représentant ne porte pas atteinte aux responsabilités du responsable du traitement ou du sous-traitant. Ce représentant doit donc accomplir ses tâches conformément à son mandat.

La portée juridique des responsabilités du représentant doit néanmoins être encore précisée par le CEPD notamment au regard des propositions présentées dans le « Guidelines 3/2018 on the territorial scope of the GDPR ».