Quelles qualifications pour les acteurs de l’informatique en nuage (cloud) ?

28.5.2026 - | Commission Nationale de l'Informatique et des Libertés

Avant de traiter des données personnelles, il est essentiel que les acteurs identifient leurs rôles. La CNIL fournit des orientations pour aider ceux du secteur de l’informatique en nuage (cloud) à identifier leurs responsabilités avec des exemples concrets.

Les difficultés liées à la qualification dans le secteur de l’informatique en nuage

La qualification des acteurs au sens du RGPD (responsable du traitement, responsable conjoint ou sous-traitant) a un impact important sur la répartition des responsabilités de chacun, notamment en termes de contractualisation, de sécurité des données et d’exercice des droits par les personnes concernées.

Dans l’écosystème de l’informatique en nuage (*cloud*), qualifier les parties peut être complexe :

- Il existe plusieurs types d’offres (infrastructure (IaaS), plateforme (PaaS) et logiciel (SaaS)) avec une répartition des responsabilités qui peut varier selon le **niveau de contrôle** du fournisseur et les **possibilités de paramétrage** du client.
- De nombreux acteurs de tailles différentes proposent plusieurs services distincts, pour lesquels la répartition des responsabilités peut évoluer avec l’avancement d’un projet donné ou des changements de besoins du client.

Pour aider les acteurs à mieux comprendre leur rôle et leurs obligations, la CNIL propose des grandes orientations – sur la base des critères dégagés par le Comité européen de la protection des données (CEPD) – couvrant trois finalités :

- la fourniture du service ;
- l’amélioration du service ;
- la sécurité « du » nuage et « dans » le nuage.

Cette grille de lecture **peut toutefois être adaptée pour bien refléter la réalité de la relation entre le fournisseur et le client**. En cas de doute, il est important de documenter la réflexion qui a été menée pour aboutir à cette qualification et d’être en mesure de la justifier.

La fourniture du service

Il s’agit des traitements de données personnelles nécessaires à la mise à disposition du service d’informatique en nuage, par le prestataire, pour le compte de son client.

Le client, responsable du traitement

En principe, **le client est responsable des traitements qu’il met en œuvre sur le service d’informatique en nuage**. En effet, il détermine :

- **les finalités (ou objectifs) des traitements de données réalisés** via le service (par exemple, gestion de la relation client via un logiciel de gestion de la relation client (CRM) ; exemple détaillé plus bas) ;
- **les moyens essentiels du traitement** dans la mesure où :
    - il dispose de la liberté du choix de son prestataire, après avoir pris connaissance de son offre de service ;
    - il conserve une marge de manœuvre dans l'utilisation et le paramétrage du service fourni par le prestataire (choix des données traitées, effacement des données, sauvegardes locales, etc.).

Le rôle du fournisseur : un sous-traitant, en principe

Le fournisseur intervient alors généralement comme sous-traitant puisqu'il va généralement traiter les données (stockage, etc.) sur les instructions de son client dans le cadre de la fourniture de son service.

À noter : le fait que le fournisseur décide de la plupart des moyens essentiels du traitement ne suffit pas à le qualifier de responsable du traitement.

Exemple : La gestion d'un logiciel de relation client (*Customer Relationship Management* - CRM)

Une entreprise utilise un logiciel CRM basé sur l'informatique en nuage pour centraliser et gérer ses interactions avec ses clients (prospection, relance, envoi de courriels). Le fournisseur de CRM stocke les données sur ses serveurs et en assure la maintenance.

Le client (entreprise utilisatrice) est responsable du traitement, car il détermine pourquoi et comment les données de ses propres clients sont utilisées (suivi commercial). Le fournisseur de CRM est sous-traitant, car il exécute uniquement les instructions nécessaires au fonctionnement du CRM, selon les instructions du client.

Dans certaines situations, **le fournisseur pourra être regardé comme co-responsable du traitement et non simple sous-traitant** : c'est notamment le cas lorsque certaines opérations de traitement servent à la fois les finalités du client et celles du fournisseur, même si les traitements mis en œuvre par la suite peuvent relever de la responsabilité propre de chaque partie.

Exemple : Traceurs et responsabilité conjointe entre client et fournisseur

Un fournisseur d'une plateforme SaaS dépose des traceurs qui collectent de données de navigation à la fois pour mesurer l'audience du site web du client et pour améliorer son propre service.

Dans ce cas, l'opération (l'utilisation de traceurs) peut relever d'une responsabilité conjointe dès lors que le client et le fournisseur contribuent ensemble à la définition des finalités et des moyens mis en œuvre pour parvenir à ces finalités. En revanche, chacun reste responsable des traitements qu'il réalise ensuite à partir de ces données pour ses propres finalités.

L’amélioration du service

L’amélioration du service proposé est une **finalité (ou objectif) fréquente** pour les fournisseurs d’informatique en nuage. Un prestataire peut traiter les données de ses clients pour identifier les difficultés techniques qu’ils rencontrent et optimiser le fonctionnement de son service.

La qualification des acteurs dépend d’une **analyse au cas par cas**. **Trois cas de figure** peuvent être distingués.

Cas n°1 : le fournisseur est responsable du traitement

Le fournisseur d’informatique en nuage peut être considéré comme responsable du traitement relatif à l’amélioration du service s’il détermine seul à la fois la **finalité** et les **moyens** du traitement.

Les indices ci-dessous peuvent aider à retenir cette qualification :

- L’amélioration du service est faite à **l’initiative du fournisseur** pour ses **propres besoins**. Le client ne profite donc qu’indirectement de l’amélioration du service.
- Le client **n’a pas connaissance** dans les **détails** du service à améliorer et de l’amélioration recherchée par le fournisseur, et n’est pas en capacité de donner des instructions au fournisseur de service.
- Le fournisseur détermine seul **les données dont il a besoin** pour améliorer ses services, et les modalités de leur traitement (comment les analyser, voire les agréger et/ou les anonymiser).
- Le traitement est fondé sur la base des **données générées par plusieurs clients** d’un même fournisseur.

Exemple : L’analyse des usages pour améliorer le service

Un fournisseur de service souhaite améliorer l’expérience utilisateur de sa plateforme SaaS de stockage, après avoir identifié que la fonctionnalité « recherche de fichiers » pose des difficultés à certains de ses clients.

Pour identifier les améliorations à apporter, il analyse des données d’utilisation de nombreux clients, telles que la fréquence d’usage, les actions réalisées ou encore le temps nécessaire pour retrouver un fichier.

Dans ce cas, le fournisseur SaaS agit en tant que responsable du traitement **dès lors qu’il détermine la finalité et les moyens de ce traitement d’amélioration du service**.

Cas n°2 : le client est responsable du traitement et le fournisseur sous-traitant

Cette hypothèse correspond au cas où le client définit l’amélioration recherchée et les moyens pour l’atteindre. Le fournisseur d’informatique en nuage donne les moyens au client de parvenir à son objectif, mais il n’a pas d’objectif propre.

Les indices ci-dessous peuvent aider à retenir ces qualifications :

- L’amélioration du service est **spécifiquement recherchée** pour le service fourni à un client en **particulier**. Le traitement visant à améliorer le service profite surtout à ce client.
- Le client détermine le **service à améliorer** et l’**amélioration** recherchée.
- Le fournisseur de service permet à son client de déterminer les moyens essentiels du traitement, y compris les **catégories de données traitées**.
- Le client est en mesure de donner des **instructions** au fournisseur qui mettra en œuvre les traitements pour atteindre l’objectif.
- Le traitement relatif à l’amélioration du service est fondé sur les **données générées par ce seul client**.

Exemple : Optimiser la performance d’une application bancaire à la demande du client

Une banque fait appel à un fournisseur de service d’informatique en nuage pour héberger son application mobile.

Suite à de nombreux retours négatifs sur la lenteur d’utilisation de l’application bancaire, elle demande au fournisseur d’en améliorer la performance.

Pour cela, la banque lui demande d’analyser certaines données, notamment des données d’usage (fréquence d’accès aux comptes, actions réalisées par les utilisateurs, etc.) afin d’optimiser le service.

Dans ce cas, la banque peut être considérée comme responsable du traitement **dès lors qu’elle fixe l’objectif et les modalités du traitement de données**. Le fournisseur agit alors comme sous-traitant en mettant en œuvre ces analyses pour le compte de la banque et selon ses instructions.

Cas n°3 : le client et le fournisseur sont responsables conjoints du traitement

Les **objectifs** et **caractéristiques** essentielles du traitement visant à améliorer le service peuvent être décidés conjointement par le client et le fournisseur d’informatique en nuage, car ce traitement présente un intérêt pour chacune des parties. Dans ce cas, le client et le fournisseur doivent être qualifiés de responsables conjoints du traitement.

Exemple : Une collaboration client-fournisseur pour adapter le service au secteur de l’énergie

Une entreprise de vente en ligne spécialisée dans la fourniture et la maintenance d’équipements énergétiques utilise une plateforme SaaS standard de gestion des « tickets » pour son service après-vente.

En raison de la nature des produits, certains tickets peuvent concerner des situations critiques pour les clients : pannes d’équipements, dysfonctionnements ou demandes urgentes d’assistance technique. La priorisation des demandes doit donc intégrer des critères spécifiques, comme l’urgence d’intervention, l’impact sur la continuité du service, ou les engagements contractuels.

L’entreprise et le fournisseur décident alors d’adapter et d’optimiser ensemble le processus de priorisation des tickets pour le secteur de l’énergie. Cette évolution bénéficie :

- à l'entreprise, pour améliorer son service après-vente ;
- au fournisseur, en lui offrant la possibilité d'adapter sa solution pour un nouveau marché.

L'entreprise définit, avec le fournisseur, les données issues de ses tickets pouvant être utilisées (catégories de demandes, délais de traitements, actions réalisées par les collaborateurs du service après-vente, niveau de satisfaction des demandeurs, etc.). Ils déterminent également conjointement les critères de priorité (priorité élevée, moyenne ou basse) et testent les évolutions du service.

Dans ce cas, **la finalité (optimiser le processus de priorisation des tickets) et les moyens essentiels (catégories de données utilisées) étant définis conjointement**, une responsabilité conjointe peut être retenue.

La sécurité du service et des traitements de données personnelles

Faire la distinction entre la sécurité « du » nuage et la sécurité « dans » le nuage

Sécurité « du » nuage et sécurité « dans » le nuage

Dans cet écosystème, il est en général possible de distinguer deux types de mesures :

- **La sécurité « du » nuage** : elle regroupe les mesures mises en œuvre par le fournisseur pour protéger son service (composants physiques, serveurs, réseaux, systèmes d'exploitation, ou applications). Cela inclut, par exemple, le contrôle d'accès aux salles serveurs, la maintenance des centres de données, les correctifs de sécurité ou encore la configuration de filtrage réseau. En principe, ces mesures ne sont pas spécifiques à un client et les clients n'interviennent pas directement dans leur mise en œuvre ni leur administration.

Exemple – La sécurisation d'une infrastructure IaaS face aux attaques réseau

Un fournisseur IaaS déploie des systèmes de détection d'anomalies sur ses réseaux internes afin de limiter la propagation d'une attaque à l'ensemble de son infrastructure, en s'appuyant notamment sur le mécanisme d'isolation logique des environnements clients.

- **La sécurité « dans » le nuage** : elle correspond aux mesures mises en œuvre par le client pour sécuriser les données hébergées sur le service, parfois via des outils fournis par le prestataire ou un fournisseur tiers. Il peut s'agir notamment du chiffrement des données en base ou de la gestion des accès et des identités. Ces mesures sont donc susceptibles d'être mises en œuvre de manière différente par les différents clients d'un même fournisseur.

Exemple : Le contrôle des accès et chiffrement des données dans un SaaS

Une entreprise utilisant un logiciel de type SaaS de gestion des ressources humaines limite l'accès aux données traitées selon les profils habilités et chiffre les données avec une gestion interne des clés assurant son contrôle exclusif.

Des responsabilités partagées en matière de sécurité qui s'articulent entre elles

La sécurité « du » nuage et la sécurité « dans » sont étroitement liées. Elles sont toutes deux nécessaires pour assurer la sécurité des traitements de données personnelles :

Une faille dans la sécurité « du » nuage peut compromettre la sécurité « dans » le nuage, malgré les mesures prises par les clients.

Exemple : Une vulnérabilité serveur rend inefficace la sécurité des données clients

Un fournisseur d'une solution SaaS n'a pas corrigé une vulnérabilité critique sur ses serveurs et permet à un attaquant d'accéder aux bases de données hébergées, rendant inopérants les dispositifs de sécurité mis en place par une entreprise utilisatrice (authentification double-facteur, un contrôle d'accès robuste).

À l'inverse, un défaut de sécurité « dans » le nuage côté client peut fragiliser l'ensemble du système en augmentant la surface d'attaque.

Exemple : Une mauvaise configuration par un client fragilise une plateforme PaaS

Une grande entreprise héberge un portail de formation sur une infrastructure PaaS mutualisée où chaque salarié peut suivre son parcours de compétences. Par erreur, elle laisse une interface d'administration accessible depuis Internet, sans restriction d'adresse IP.

Un attaquant qui compromet ce compte peut lancer des attaques par déni de service distribué (*Distributed Denial of Service attack* ou DDoS en anglais) ou déployer des programmes malveillants, affectant la sécurité globale de la plateforme ou la disponibilité des ressources partagées avec les autres clients du PaaS.

Les qualifications des acteurs pour la sécurité « du » nuage

Cas n°1 : les données personnelles des employés du fournisseur

De manière générale, le **fournisseur est responsable du traitement des données personnelles de ses employés** lorsqu'elles sont traitées aux fins d'assurer la sécurité « du » nuage.

Exemple : La responsabilité du fournisseur pour la traçabilité des accès de son administrateur

Un administrateur du fournisseur se connecte à son compte professionnel pour déployer un correctif de sécurité sur l'infrastructure. Cette opération bénéficie à l'ensemble des clients hébergés sur l'infrastructure. Les identifiants de l'administrateur, l'heure de connexion, son adresse IP et les actions effectuées sont enregistrées dans des journaux pour en garantir la traçabilité et la détection d'éventuels abus. Dans ce cadre, le fournisseur agit en tant que responsable du traitement des données de son employé pour la finalité de sécurité « du » nuage.

Exemple : La responsabilité du fournisseur pour le contrôle des accès de son employé

Un employé du fournisseur accède à une salle serveur hébergeant des équipements critiques, comme les modules de gestion des clés de chiffrement (module de sécurité matériel, *Hardware Security Module* ou HSM). Le système de contrôle d'accès vérifie ses habilitations et enregistre son identité, sa fonction, ses droits d'accès ainsi que la date et l'heure de l'accès. Dans ce cas, **le fournisseur est le responsable du traitement des données personnelles de son employé pour la sécurité « du » nuage.**

Cas n°2 : les données personnelles des clients qui utilisent le service

Ce cas ne concerne en principe pas les données que le client héberge pour ses propres finalités métiers (dossiers RH, base de données de clients ou de patients, etc.) mais les données personnelles générées ou collectées lors de l'usage technique du service, lorsque ces données sont utilisées par le fournisseur pour sécuriser son infrastructure, protéger les clients contre les attaques et maintenir la disponibilité du service.

Plusieurs catégories de données personnelles peuvent être concernées :

- **des données d'identification et de compte** : noms, prénoms, adresses électroniques, identifiants de compte, etc.

Exemple : Le traitement des données d'authentification du client pour sécuriser le service

Une grande entreprise héberge une application métier sur une plateforme IaaS et donne un accès à un administrateur à la console d'administration sur la plateforme. Le fournisseur traite son adresse électronique professionnelle, ses identifiants, son rôle et les informations utilisées pour l'authentification multifacteur. Ces données permettent de prévenir et de détecter la compromission d'un compte administrateur, à privilèges élevés, et de protéger l'infrastructure globale du service.

- **des données de connexion et de journalisation** : adresses IP, horodatage des connexion, journaux (*logs*) administrateur, etc.

Exemple : La journalisation des connexions pour détecter des attaques sur l'infrastructure

Une entreprise dispose de plusieurs machines virtuelles sur la même plateforme IaaS. Chaque connexion à la console de la plateforme est enregistrée (adresse IP, date et heure de la connexion, actions réalisées). Le fournisseur peut ainsi repérer des comportements suspects, comme une vague de connexions depuis la même adresse IP, et prévenir des attaques sur l'infrastructure globale.

Cette journalisation à des fins de sécurité « du » nuage se distingue de celle mise en œuvre pour le compte d'un client spécifique qui relève de la sécurité « dans » le nuage.

- **des données de télémétrie et de diagnostic** : fréquence et volume des requêtes, consommation de ressources, etc.

Exemple : La détection d'activités anormales via la télémétrie

Une entreprise utilise un logiciel SaaS de facturation. Les collaborateurs s'y connectent via un navigateur. Le fournisseur collecte des données de télémétrie liées à l'usage du service : fréquence de requêtes envoyées depuis un compte donné, type d'actions réalisées, version du navigateur utilisé, témoins de connexion (*cookies*) techniques, etc. Ces données permettent de détecter un comportement anormal, par exemple en cas de compromission de compte, et de protéger l'infrastructure globale.

- **des données liées à la surveillance de l'usage des ressources réseau.**

Exemple : La détection de minage pirate via le suivi d'utilisation des ressources

Une entreprise utilise une solution PaaS pour ses applications. Le fournisseur mesure la consommation de ressources (puissance de calcul, mémoire, bande passante) en associant ces informations aux identifiants des comptes qui hébergent les applications. Cela permet de détecter des usages suspects comme une consommation de ressources anormalement élevée, pouvant révéler une activité de type « minage pirate » (ou *cryptojacking*, c'est-à-dire l'acte de détourner des ressources informatiques pour extraire des crypto-monnaies à l'insu des utilisateurs). Le traitement assure la sécurité « du » nuage en permettant la détection précoce de l'incident et ainsi d'isoler la machine concernée, protégeant ainsi les ressources globales de la plateforme.

En règle générale, **le fournisseur peut être qualifié de responsable du traitement pour les données personnelles traitées pour assurer la sécurité « du » nuage.**

Les indices ci-dessous peuvent aider à retenir cette qualification :

- **le traitement bénéficie à l'ensemble des clients** et participe à la sécurité globale du service et non celle d'un client en particulier ;
- **la finalité de sécurité « du » nuage est définie par le fournisseur uniquement** ;
- **le fournisseur dispose des compétences techniques et, en règle générale, de l'accès aux données nécessaires** et détermine les moyens essentiels du traitement, notamment les données à traiter.

Exemple : Le fournisseur, responsable du traitement de détection d'anomalies au sein de son service

Le fournisseur IaaS peut être amené à traiter des données personnelles contenues dans les journaux (*logs*) de connexion pour détecter globalement des anomalies dans l'accès à son infrastructure. Bien qu'ils puissent être autorisés par les clients dans le cadre d'un contrat, ces traitements ne répondent pas à un besoin spécifique d'un client et ne sont pas réalisés sur instruction.

La finalité (détection des anomalies) est déterminée par le fournisseur qui détermine également des données collectées, les modalités de journalisation et les seuils d'alerte et de détection. Le client n'intervient pas dans ces choix techniques.

Le fournisseur est donc responsable du traitement des données contenues dans les journaux pour sécuriser l'infrastructure dans son ensemble.

Néanmoins, cette analyse peut varier selon le service (IaaS, PaaS ou SaaS) ou le rôle du client. En effet, dans certaines configurations, une responsabilité conjointe est possible notamment lorsqu'un

client impose des exigences de sécurité spécifiques qui affectent la gestion de la sécurité globale du service.

Exemple : Responsabilité conjointe pour la finalité de sécurité du nuage

Un grand groupe industriel utilise une offre IaaS pour héberger des applications critiques.

Contrairement à un client standard, l'entreprise impose au fournisseur des exigences de sécurité très précises au moment de la négociation du contrat (types de journaux, seuils d'alerte, blocage automatique de certaines plages d'adresses IP, plan de continuité ou de reprise d'activité spécifique, etc.).

Dans ce cas, le traitement des données (identifiants des administrateurs, les adresses IP, les horodatages, les actions réalisées sur les instances du service, etc.) vise à protéger à la fois les systèmes d'information du client et l'infrastructure globale de la plateforme IaaS. Par ailleurs, dans une telle configuration, le client influence directement les moyens du traitement.

Dès lors, une responsabilité conjointe peut être retenue.

Les qualifications des acteurs pour la sécurité « dans » le nuage

Dans la plupart des cas, **le client est responsable du traitement** réalisé dans le nuage. Les mesures de sécurité peuvent être intégrées au traitement principal. Elles peuvent alternativement constituer un traitement distinct, avec pour finalité d'assurer la protection du système d'information ou des applications qu'il héberge dans le nuage. Dans ce cadre, **le fournisseur intervient comme sous-traitant** et assiste le client pour mettre en œuvre les mesures de sécurité appropriées.

Exemple : Le client est responsable du traitement et des mesures de sécurité mises en œuvre

Une entreprise de commerce en ligne héberge sa base clients sur une plateforme SaaS.

Le fournisseur met à disposition des outils et de fonctionnalités de sécurité (chiffrement des données au repos et en transit, gestion des identités et des accès, journalisation des événements, dispositifs de sauvegarde, etc.).

L'entreprise active certaines de ces fonctionnalités et en définit les paramètres : elle active le chiffrement des données au repos et en transit, elle configure les accès et les profils d'habilitation, organise la journalisation et les sauvegardes. Ces mesures impliquent des traitements de données personnelles des utilisateurs finaux (identifiants, journaux, adresses IP, traces d'accès, etc.) pour assurer la sécurité « dans » le nuage.

Dans ce cas, l'entreprise est responsable de ces traitements **car elle en détermine les finalités et les moyens**. Le fournisseur agit comme sous-traitant **en mettant en œuvre ces mesures pour le compte et selon les instructions de l'entreprise**.

https://www.cnil.fr/fr/quelles-qualifications-pour-les-acteurs-de-linformatique-en-nuage-cloud