arcep
autorité de régulation
des communications électroniques,
des postes et de la distribution de la presse

RÉPUBLIQUE FRANCAISE

GUIDE PRATIQUE

Demande de LABELLISATION en tant que prestataire de services d'intermédiation de données reconnu dans l'Union européenne

22 mai 2024

ISSN n°2258-3106

Demande de labellisation en tant que prestataire de services d'intermédiation de données reconnu dans l'Union européenne

Guide de la démarche

1 Cadre réglementaire de la labellisation

Le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données établit notamment, conformément au paragraphe 9 de l'article 11, la possibilité pour les prestataires de services d'intermédiation de données de demander, auprès de l'autorité compétente dont ils relèvent, à obtenir le label « prestataire de services d'intermédiation de données reconnu dans l'Union ». Si, au terme de l'instruction de la demande, l'autorité compétente estime que le prestataire satisfait aux conditions requises par l'article 12 du règlement, celui-ci pourra alors utiliser ce label dans ses communications écrites et orales, ainsi qu'un logo associé.

L'autorité compétente est celle du pays où se situe votre établissement principal ou votre représentant légal. Pour la France, la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique dispose dans son article 36 que l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) « *est l'autorité compétente en matière de services d'intermédiation de données, en application de l'article 13 du règlement (UE) 2022/868* ».

À ce titre, les prestataires de services d'intermédiation de données de peuvent réaliser cette demande de labellisation auprès de l'Arcep, selon la procédure décrite par ce document.

2 Dépôt des dossiers de demande

Les prestataires de services d'intermédiation de données pourront soumettre à l'Arcep un dossier de demande afin d'obtenir le label « prestataire de services d'intermédiation de données reconnu dans l'Union ». Une liste de pièces justificatives indicative que le prestataire de services d'intermédiation de données devra fournir afin que l'Arcep puisse instruire sa demande au regard des conditions prévues par l'article 12 du règlement est disponible dans l'annexe I du présent document.

Ces dossiers devront être transmis à l'adresse intermediation_donnees@arcep.fr, par exemple grâce à l'outil en ligne France transfert**.**

3 Instruction des dossiers

Une fois le dossier complet transmis, les services de l'Arcep procèderont alors à l'instruction du dossier. Des compléments d'information peuvent être demandés lors de cette instruction. En outre, comme prévu par la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique, l'Arcep transmettra à la Commission nationale de l'informatique et des libertés les éléments du dossier de demande permettant au président de la Commission nationale de l'informatique et des libertés de fournir ses éventuelles observations sur les questions liées à la protection des données à caractère personnel.

4 Traitement des données

Vos données personnelles sont collectées sous la responsabilité de l'Arcep pour le respect d'une obligation légale au sens du e) de l'article 6 du règlement général (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données (RGPD).

Vos données sont collectées, traitées et conservées dans le cadre du processus de demande de labellisation prévu à l'article 11 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données.

Les dossiers de labellisation incomplets et leurs données seront supprimés 6 mois après la date de dépôt initiale auprès de l'Arcep. Seules les données de contact seront conservées par l'Arcep tout au long de l'activité du prestataire pour l'exercice des missions de l'Arcep.

Sont destinataires de vos données, dans le cadre de leurs attributions et dans la limite du besoin d'en connaître, les personnes chargées d'instruire les demandes de notification au sein de l'Arcep.

Ces informations pourront par ailleurs être transmises à la Commission nationale de l'informatique et des libertés dans le cadre de la procédure prévue à l'article 38 de la loi n°2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique.

Vous pouvez exercer vos droits d'accès, de rectification, de limitation, d'opposition en vous adressant au délégué à la protection des données de l'Arcep à l'adresse suivante : donneespersonnelles@arcep.fr.

Après avoir contacté le délégué à la protection des données, si vous estimez que vos droits Informatique et Libertés ne sont toujours pas respectés, vous pouvez faire, conformément au RGPD et à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, une réclamation en ligne ou par voie postale :

CNIL - Service des Plaintes
3 Place de Fontenoy
TSA 80715
75334 Paris Cedex 07

5 Contacts

Pour toute question relative à cette procédure vous pouvez vous adresser à l'Arcep en envoyant un courrier électronique à l'adresse suivante : intermediation_donnees@arcep.fr.

6. Rappel de la réglementation sur la protection des données personnelles

Le règlement sur la gouvernance sur les données s'entend sans préjudice de l'obligation qui est faite aux prestataires de services d'intermédiation de données de respecter le règlement (UE) 2016/679, dit règlement général sur la protection de données (RGPD).

A ce titre, comme toute organisation amenée à collecter et traiter des données personnelles, les prestataires de services d'intermédiation de données sont soumis à l'ensemble des obligations du RGPD. Ils doivent notamment créer et tenir à jour un registre des traitements de données, informer les personnes et le cas échéant recueillir leur consentement, sécuriser les données, faciliter et répondre à l'exercice des droits des personnes. Les PSID pourront réaliser une analyse d'impact relative à la protection des données (AIPD) - toujours conseillée, obligatoire pour certains types de traitement. Ils devront, dans certains cas, nommer un délégué à la protection des données.

Annexe I

La présente annexe constitue une liste indicative de pièces justificatives susceptibles d'être transmises à l'Arcep afin d'apprécier si la demande répond aux conditions prévues à l'article 12 du règlement sur la gouvernance des données. Pour les besoins de l'instruction de la demande, l'Arcep peut demander la communication de tout autre document pertinent.

Référence	Exigences du DGA (Chapitre III, Art. 12)	Justificatifs potentiels
Art 12, a)	Le prestataire de services d'intermédiation de données ne peut pas utiliser les données pour lesquelles il fournit des services d'intermédiation de données à des fins autres que leur mise à disposition des utilisateurs de données, et il fournit les services d'intermédiation de données par l'intermédiaire d'une personne morale distincte ;	Conditions générales d'utilisation (CGU) du service ; Description des mesures de gestion des accès ; Statuts de l'entreprise ; Structure de propriété.
Art. 12, b)	les modalités commerciales, y compris la tarification, de la fourniture de services d'intermédiation de données à un détenteur de données ou à un utilisateur de données ne doivent pas être subordonnées au fait que le détenteur de données ou l'utilisateur de données utilise ou non d'autres services fournis par le même prestataire de services d'intermédiation de données ou par une entité liée, et dans l'affirmative, à la mesure dans laquelle le détenteur de données ou l'utilisateur de données utilise ces autres services ;	Conditions générales d'utilisation (CGU) du service ; Conditions générales de vente (CGV) ; Liste de services accessoires du PSID et ou de tiers (ex : sous-traitance).
Art. 12, c)	les données collectées en ce qui concerne toute activité d'une personne physique ou morale aux fins de la fourniture d'un service d'intermédiation de données, notamment la date, l'heure et les données de géolocalisation, la durée de l'activité et les connexions établies avec d'autres personnes physiques ou morales par la personne qui utilise le service d'intermédiation de données	CGU ; Description des finalités de réutilisations prévues ; Description des procédures et mesures préventives contre les réutilisations non autorisées ;

	ne doivent être utilisées que pour le développement dudit service d'intermédiation de données, ce qui peut impliquer l'utilisation de données pour la détection de fraudes ou pour la cybersécurité, et sont mises à la disposition des détenteurs de données sur demande ;	Description de la procédure de demande d'accès aux données, et procédure de réponse prévue ; Echantillon de journaux d'accès aux métadonnées.
Art. 12, d)	le prestataire de services d'intermédiation de données facilite l'échange des données au format dans lequel il les reçoit d'une personne concernée ou d'un détenteur des données, ne convertit les données dans des formats spécifiques que pour améliorer l'interopérabilité intra sectorielle et transsectorielle, ou si l'utilisateur de données le demande, ou lorsque le droit de l'Union le requiert, ou pour assurer l'harmonisation avec des normes internationales ou européennes en matière de données, et donne aux personnes concernées ou aux détenteurs de données une possibilité de non-participation en ce qui concerne ces conversions, à moins que la conversion ne soit requise par le droit de l'Union ;	CGU ; Liste des données converties par défaut, formats, normes ou standards associés à ces conversions ; Description du processus de recueil de choix, quant à la possibilité de non-participation à la conversion.
Art. 12, e)	les services d'intermédiation de données peuvent prévoir de fournir aux détenteurs de données ou aux personnes concernées des instruments et services spécifiques supplémentaires dans le but particulier de faciliter l'échange de données, tels que le stockage temporaire, l'organisation, la conversion, l'anonymisation et la pseudonymisation, ces instruments étant uniquement utilisés à la demande expresse ou moyennant l'approbation expresse du détenteur de données ou de la personne concernée et les instruments de tiers proposés dans ce contexte n'étant pas utilisés à d'autres fins ;	CGU ; Liste de services complémentaires proposés aux détenteurs et aux utilisateurs de données ; Description du processus de demande ou d'approbation pour l'utilisation de services supplémentaires.

Art. 12, f)	Le prestataire de services d'intermédiation de données veille à ce que la procédure d'accès à son service soit équitable, transparente et non discriminatoire à l'égard tant des personnes concernées et des détenteurs de données que des utilisateurs de données, y compris en ce qui concerne les prix et les conditions de service ;	CGU/CGV, y compris les conditions tarifaires d'accès au service ; Description du modèle d'affaire.
Art. 12, g)	Le prestataire de services d'intermédiation de données met en place des procédures pour prévenir les pratiques frauduleuses ou abusives en lien avec des parties cherchant à obtenir un accès via ses services d'intermédiation de données ;	Analyse de risque (voir Annexe II) et description des procédures de prévention ; Eventuelles certifications ; Eventuelles restitutions d'audits.
Art. 12, h)	en cas d'insolvabilité, le prestataire de services d'intermédiation de données assure une continuité raisonnable de la fourniture de ses services d'intermédiation de données et, lorsque ces services d'intermédiation de données assurent le stockage de données, il met en place des mécanismes pour permettre aux détenteurs de données et aux utilisateurs de données d'avoir accès à leurs données, de les transférer ou de les extraire et, lorsque ces services d'intermédiation de données sont fournis entre des personnes concernées et des utilisateurs de données, pour permettre aux personnes concernées d'exercer leurs droits;	CGU, CGV ; Description des mesures anticipatoires permettant aux détenteurs et utilisateurs de données l'accès, le transfert ou l'extraction des données en cas d'insolvabilité ; Lorsque ces services d'intermédiation de données sont fournis entre des personnes concernées et des utilisateurs de données, description des mesures permettant aux personnes concernées d'exercer leurs droits en cas d'insolvabilité.
Art. 12, i)	Le prestataire de services d'intermédiation de données prend les mesures appropriées pour assurer l'interopérabilité avec d'autres services d'intermédiation de données, entre autres au moyen de normes ouvertes communément utilisées dans le	Liste des secteurs dans lequel le PSID opère et des normes ouvertes communes correspondantes ;

	secteur dans lequel le prestataire de services d'intermédiation de données exerce ses activités ;	Liste des mesures mises en œuvre pour assurer l'interopérabilité avec d'autres services ; Eventuelles certifications ; CGU.
Art. 12, j)	Le prestataire de services d'intermédiation de données met en place des mesures techniques, juridiques et organisationnelles appropriées afin d'empêcher le transfert de données à caractère non personnel ou l'accès à celles-ci dans les cas où ils sont illicites au regard du droit de l'Union ou du droit national de l'État membre concerné ;	Analyse de risque de transferts (voir Annexe II) et description des mesures techniques, juridiques et organisationnelles associées ; CGU, CGV ; Eventuelles certifications ; Eventuels restitutions d'audits.
Art. 12, k)	Le prestataire de services d'intermédiation de données informe sans retard les détenteurs de données en cas de transfert, d'accès ou d'utilisation non autorisés portant sur les données à caractère non personnel qu'il a partagées ;	Description des procédures de détection et de traitement des accès et usages non autorisés ; Description du canal d'information ; CGU.
Art. 12, l)	Le prestataire de services d'intermédiation de données prend les mesures nécessaires pour garantir un niveau de sécurité approprié pour le stockage, le traitement et la transmission de données à caractère non personnel, et le prestataire de services d'intermédiation de données garantit également le niveau de sécurité le plus élevé pour le stockage et la transmission d'informations sensibles sous l'angle de la concurrence ;	Analyse de risque (voir Annexe II) ; Description des mesures de sécurité ; Eventuelles certifications ; Eventuels restitutions d'audits.

Art. 12, m)	le prestataire de services d'intermédiation de données proposant des services à des personnes concernées agit au mieux de leurs intérêts lorsqu'il facilite l'exercice de leurs droits, notamment en informant et, le cas échéant, en conseillant les personnes concernées de manière concise, transparente, compréhensible et aisément accessible sur les utilisations prévues des données par les utilisateurs de données et sur les conditions générales applicables à ces utilisations, avant que les personnes concernées ne donnent leur consentement;	CGU ; Politique de confidentialité (Mentions d'information RGPD).
Art. 12, n)	lorsqu'un prestataire de services d'intermédiation de données fournit des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données, il précise, le cas échéant, la juridiction des pays tiers où l'utilisation des données est prévue et fournit aux personnes concernées des outils permettant à la fois de donner et de retirer leur consentement et aux détenteurs de données des outils permettant à la fois de donner et de retirer l'autorisation de traiter des données;	CGU ; Politique de confidentialité ; Description de la gestion des autorisations et du consentement et visualisation (granularité, design du choix). Information sur l'exercice des droits.
Art. 12, o)	Le prestataire de services d'intermédiation de données tient un journal de l'activité d'intermédiation de données.	Journal de bord de l'activité d'intermédiation de données (Description et/ou modèle schématique en cas d'activité non démarrée).

Annexe II

Certaines conditions énoncées à l'article 12 du règlement sur la gouvernance des données, notamment celles relatives :

- à la prévention des pratiques frauduleuses ou abusives en lien avec des parties cherchant à obtenir un accès via ses services d'intermédiation de données (Article 12, g) ;
- à la prévention des transferts de données à caractère non personnel ou l'accès à celles-ci dans les cas où ils sont illicites au regard du droit de l'Union ou du droit national de l'État membre concerné (Article 12, j) ;
- à la mise en place de mesures nécessaires afin de garantir un niveau de sécurité approprié pour le stockage, le traitement et la transmission de données à caractère non personnel, en particulier pour les informations sensibles sous l'angle de la concurrence (Article 12, l),

appellent de manière générale à une évaluation du niveau de sécurité des données non personnelles, au regard des risques liés aux activités du prestataire de services d'intermédiation de données.

Afin de justifier du respect de ces conditions, il peut être ainsi envisagé de conduire au préalable une étude des risques auxquels l'activité de prestataire de services d'intermédiation de données est exposée et d'identifier quelles mesures préventives doivent être mises en place.

Une analyse de risque constitue la formalisation la réflexion relative à la sécurité des données, et pourrait être structurée, à titre indicatif et de manière susceptible d'évoluer, selon étapes détaillés dans la suite de ce document.

1 Recenser les traitements de données non personnelles effectués ou prévus

Identifier synthétiquement chaque traitement (stockage, transmission, conversion, etc.) considéré, notamment sa nature, son objectif, et son périmètre. Par exemple, quels processus et quels supports (locaux, matériels, logiciels, ressources cloud, etc.) constitueront l'environnement du traitement ; y compris les destinataires de données, durées jusqu'à effacement des données, les canaux de communication, (Wi-Fi, Bluetooth, appels, etc.) ?

2 Identifier les risques que ces traitements peuvent susciter

L'identification des risques que ces traitements peuvent susciter peut se faire en tenant compte :

- d'évènements redoutés liés à la sécurité des données ou à leur transfert ;
- d'impact potentiels, par exemple pour les détenteurs et les utilisateurs de données ;
- de sources rendant possible de tels évènements ;
- et de menaces susceptibles d'exploiter ces risques.

2.1 Evènements redoutés

Au regard de l'article 12 du règlement sur la gouvernance des données, il semble opportun de considérer *a minima* les évènements redoutés suivants :

- **Compromission/divulgation des données,** dont accès ou transfert illégitime des données ;
- **Modification non désirée des données ;**

- **Disparition temporaire ou définitive des données.**

2.2 Identification des impacts potentiels

Selon le contexte et l'utilisation prévue du service d'intermédiation de données, les évènements redoutés peuvent avoir des conséquences variées. Ainsi, **l'identification des impacts potentiels consiste à associer à chaque évènement redouté les conséquences** qu'il est susceptible d'avoir. Par exemple, une modification non désirée des données d'un détenteur de données est susceptible de leur faire perdre leur valeur, ou encore un accès illégitime aux données est susceptible de donner un avantage à un concurrent. Ces impacts s'apprécient au regard notamment de la concurrence, et d'après l'article 12 l), une attention particulière devra être portée sur les impacts liés aux informations sensibles sous l'angle de la concurrence.

2.3 Identification des sources de risques

Les évènements redoutés précédents sont susceptibles d'être déclenchés par différentes sources de risque, qu'il convient d'identifier. **Parmi les sources de risques pouvant rendre possible de tels évènements,** il est notamment important de tenir compte :

- des sources humaines (ex : utilisateur) et non humaines (ex : logiciel malveillant, incendie) ;
- des sources internes (ex : administrateur) et externes (ex. utilisateur, concurrent, attaquant).

2.4 Identification des menaces

En complément de l'identification des sources de risques, il convient d'identifier la manière dont les évènements redoutés sont susceptibles de se produire**, c'est-à-dire les menaces.** Par exemple :

- l'utilisation de vulnérabilités de certains supports ou contextes de traitements pour compromettre les données traitées ou rendre vos services utilisables (surcharge, déni de service, logiciel malveillant, etc.) ;
- une mauvaise utilisation du service, comme des erreurs dans la manipulation des données ;
- la perte de supports de données par oubli, vol ou détérioration.

Au regard des conditions prévues par l'article 12, il conviendra **en particulier de tenir compte :**

- des pratiques frauduleuses ou abusives pourraient avoir lieu en lien avec des parties cherchant à obtenir un accès à vos services à d'intermédiation de données (Article 12.g) ;
- de potentielles situation d'insolvabilité vous empêcherait d'assurer une continuité raisonnable de la fourniture de vos services d'intermédiation de données, et de permettre aux détenteurs aux utilisateurs de données d'y avoir accès, de les transférer ou de les extraire (Article 12.h)
- des accès et/ou des transferts des données à caractère non personnel illicites au regard du droit de l'Union ou du droit national de l'Etat membre concerné pourraient survenir (Article 12.j) ;

3 Déterminer les mesures à mettre en œuvre

Au regard des éléments identifiés précédents, il convient de déterminer et de mettre en œuvre des mesures permettant de réduire chaque risque. Ces mesures portent sont relatives tout à la fois :

- aux données elles-mêmes : par exemple le chiffrement, la traçabilité des traitements et le contrôle des accès,
- à la sécurité du système dans lequel les données sont traitées : sauvegardes, gestion des postes de travail, maintenance, sécurité des réseaux, contrôles des accès physiques, etc.
- à la gouvernance de l'organisation : par exemple des ressources suffisantes, une politique de gestion des habilitations et de formation des personnels et de traitement effectif des incidents, ou un encadrement des traitements par les sous-traitants.

En outre, conformément à l'article 12, l) ces mesures devront garantir le niveau de sécurité le plus élevé pour le stockage et la transmission d'information sensibles sous l'angle de la concurrence.

4 Déterminer les risques résiduels

Au regard des mesures mises en œuvre, il est ensuite possible d'identifier la **gravité des risques**, c'est-à-dire de leurs impacts et du préjudice potentiel causé par les évènements redoutés associés, et leur **vraisemblance** (probabilité qu'ils se réalisent). Ces deux indicateurs peuvent par exemple être rapportés à une échelle indicative de risque (négligeable, modéré, important, maximal).

Sur cette base, il sera possible :

- d'évaluer ces mesures existantes ou prévues ;
- de mobiliser cette évaluation pour identifier les compléments nécessaires ;
- et de structurer des démarches d'amélioration continue. Par exemple pour prioriser les risques les plus graves et les plus vraisemblables au regard de l'évolution des menaces ou du profil de risque du service d'intermédiation de données.

5 Mettre à profit les synergies possibles entre ces démarches

Les mesures prises pour évaluer et maîtriser les risques de vos activités peuvent en combinaison contribuer à répondre aux autres conditions de l'article 12.

Par exemple, la tenue d'un journal de l'activité d'intermédiation de données, à laquelle sont tenus tous les PSID (article 12, o) devrait pouvoir contribuer aussi à votre capacité à :

- détecter les fraudes et abus que l'article 12.g vous impose d'inclure parmi vos préoccupations ;
- détecter les incidents, les traiter et les notifier sans retard aux intéressés (article 12. k).

Le cas échéant, votre demande de labellisation peut être complétée par des éléments réalisés en application d'autres cadres pertinents. Il peut s'agir par exemple, des certifications dont les approches seraient compatibles, ou d'analyses d'impact effectuées au titre du RGPD.

Ainsi, des analyses et des mesures techniques, juridiques et organisationnelles pour empêcher les accès et transferts de données illicites au sens de l'Article 12.j, pourraient bénéficier en partie à celles qui s'imposent pour la protection des données personnelles.

En outre, des vérifications croisées pourraient être nécessaires dans le cas de données personnelles et non personnelles inextricablement liées.

Enfin, il est important de rappeler que le règlement européen sur la gouvernance des données ne crée pas de nouvelle base légale pour le traitement de données personnelles, et s'applique sans préjudice de l'exercice de leurs pouvoirs respectifs par les autorités compétentes en matière de cybersécurité, de protection des données, de concurrence ou de sectorielles (Article 13.3).