
ACCORD-CADRE 2024-0319

**Réalisation et maintien en conditions opérationnelle et
de sécurité du service de garantie de l'identité
numérique (SGIN)**

**CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIÈRES (CCAP)
ANNEXE 1
CONDITIONS DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL**

SOMMAIRE

1. DEFINITIONS SPECIFIQUES AUX DONNEES A CARACTERE PERSONNEL	4
2. OBJET ET CHAMP D'APPLICATION	5
3. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT	5
3.1. Instructions	5
3.2. Limitation de la finalité	6
3.3. Confidentialité des données	6
3.4. Mesures de sécurité des traitements	6
3.5. Documentation et conformité	6
3.6. Recours à des Sous-traitants ultérieurs	7
3.7. Transferts de données hors de l'Union européenne	7
3.8. Sort des données	8
3.9. Assistance au Responsable de traitement	8
3.9.1. Réponse aux demandes des personnes concernées	8
3.9.2. Notification des violations de données	8
3.9.3. Réalisation d'analyses d'impact	8
3.9.4. Consultation préalable avec l'autorité de contrôle	9
4. LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT	9
5. ANNEXE A : DESCRIPTION DU TRAITEMENT FRANCE IDENTITE	10
5.1. Catégories de personnes concernées dont les données à caractère personnel sont traitées :	10
5.2. Catégories de données à caractère personnel traitées :	10
5.3. Les données sensibles traitées et les limitations ou garanties appliquées :	10
5.4. Nature du traitement :	10
5.5. Finalités pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable de traitement :	10
5.6. Durée du traitement :	10
5.7. Traitement par les sous-traitants ultérieurs :	11
6. ANNEXE B : DESCRIPTION DU TRAITEMENT ATTESTATION FRANCE IDENTITE	11

6.1. Catégories de personnes concernées dont les données à caractère personnel sont traitées :	11
6.2. Catégories de données à caractère personnel traitées :	11
6.3. Données sensibles traitées et limitations ou garanties appliquées :	11
6.4. Nature du traitement :	11
6.5. Finalité pour laquelle les données à caractère personnel sont traitées pour le compte du responsable du traitement :	11
6.6. Durée du traitement :	11
6.7. Traitement par les sous-traitants (ultérieurs) :	12

Les présentes conditions de traitement des données personnelles se composent des parties suivantes :

Le corps du présent document, **l'Annexe n°1 du CCAP**, expose les droits et obligations du Responsable de Traitement (l'ANTS) et du Sous-traitant (le Titulaire) dans le cadre des présentes conditions de traitement des données personnelles (CTD).

- **L'Annexe A** décrit les activités du traitement Service de Garantie de l'Identité Numérique (SGIN).
- **L'Annexe B** décrit les activités du traitement Attestation France Identité (AFI).

Le périmètre du présent marché inclut des applications susceptibles de traiter des données à caractère personnel dont le traitement est encadré par la loi n°78-17 du 6 janvier 1978 dite loi « Informatique et Libertés » et par le règlement (UE) 2016/679 du 27 avril 2016 dit « RGPD ». Définitions spécifiques aux données à caractère personnel

- **Donnée à caractère personnel** : désigne toute information relative à une personne physique identifiée ou identifiable. Une « personne physique identifiable » est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro de téléphone, une adresse électronique, un numéro d'identification, des données de localisation, un identifiant en ligne, ou encore par un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- **Traitement** : désigne toute opération ou tout ensemble d'opérations effectuées sur des données à caractère personnel, qu'elles soient ou non réalisées par des moyens automatisés. Cela inclut, notamment, la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction des données.
- **Instruction** : désigne toute directive écrite émise par le Responsable de traitement et reçue par le Sous-traitant, conformément au présent Accord-cadre. Ces instructions détaillent les modalités de traitement des données à caractère personnel et sont accompagnées d'un document spécifique pour chaque fichier concerné.
- **Responsable de traitement** : désigne toute personne physique ou morale, autorité publique, service ou autre organisme qui détermine, seul ou conjointement avec d'autres, les finalités et les moyens du traitement des données. Dans le cadre du présent Accord-cadre, le Responsable de traitement est l'ANTS.
- **Sous-traitant** : désigne le Titulaire du présent Accord-cadre, à savoir la personne morale qui traite les données à caractère personnel pour le compte du Responsable de traitement, conformément à ses instructions. Le Titulaire est tenu de ne traiter ces données qu'exclusivement pour le compte de l'ANTS, en respectant les dispositions prévues dans le présent Accord-cadre.
- **Violation des données à caractère personnel** : désigne tout incident de sécurité, intentionnel ou non, d'origine malveillante ou accidentelle, entraînant une atteinte à

l'intégrité, la confidentialité ou la disponibilité des données à caractère personnel. Cela inclut, par exemple, les accès non autorisés, les pertes, les altérations ou les divulgations non autorisées de données.

1. OBJET ET CHAMP D'APPLICATION

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Titulaire, en qualité de Sous-traitant, s'engage à réaliser pour le compte de l'ANTS, Responsable de traitement, les opérations de traitement de données à caractère personnel spécifiées dans le périmètre convenu.

- **Le traitement Service de Garantie de l'Identité Numérique (SGIN)**, encadré par le décret n° 2022-676 du 26 avril 2022, constitue le moyen d'identification électronique régalién et repose sur la Carte Nationale d'Identité électronique (CNle) avec carte à puce. Grâce à un téléphone mobile compatible et l'application mobile « France identité », l'utilisateur peut s'authentifier de manière sécurisée auprès de fournisseurs de services en ligne ou générer une attestation électronique d'attributs, qu'il peut transmettre aux tiers de son choix.
- **Le traitement Attestation France Identité (AFI)**, dont l'ANTS est également responsable, a pour finalité de générer et de gérer des attestations électroniques d'attributs d'identité pour les usagers de l'application mobile France Identité. Ces attestations permettent de prouver des attributs spécifiques, tels que les droits à conduire. Elles sont sécurisées par un cachet électronique de l'État et sont destinées à être transmises ou présentées dans le cadre de démarches administratives ou de contrôles. Ce service s'inscrit dans l'écosystème du portefeuille européen d'identité numérique, en garantissant des attestations vérifiables conformes aux exigences de l'identité numérique européenne.

L'ANTS, en tant que Responsable de traitement, assume la responsabilité des deux traitements mentionnés. Les détails relatifs aux opérations de ces traitements, notamment les catégories de données à caractère personnel concernées et les finalités spécifiques, sont précisés dans les **Annexes A : Description du traitement SGIN** et **B : Description du traitement Attestation France Identité**, du présent accord-cadre.

Dans le cadre de cet accord, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement des données à caractère personnel, en particulier le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, applicable depuis le 25 mai 2018 (ci-après « RGPD »).

2. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

2.1. Instructions

Le Sous-traitant, Titulaire du présent Accord-Cadre, s'engage à se conformer aux instructions documentées du Responsable de traitement, l'ANTS, figurant au présent Accord-Cadre.

Si le Sous-traitant considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit des États membres relatif à la protection des données, il en informe immédiatement le Responsable de traitement.

Des instructions peuvent également être données ultérieurement par le Responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

2.2. Limitation de la finalité

Le Sous-traitant, s'engage à traiter les données uniquement pour les finalités définies dans les Annexes A et B du présent accord, sauf instruction complémentaire du Responsable du traitement.

2.3. Confidentialité des données

Le Sous-traitant garantit la confidentialité absolue des données à caractère personnel traitées dans le cadre du présent accord. Ces données ne peuvent être ni divulguées ni utilisées à des fins autres que celles définies dans les annexes contractuelles.

Le Sous-traitant s'engage à ce que chaque personne ayant accès aux données dans le cadre des traitements concernés soit soumise à une obligation stricte de confidentialité. Il veille également à ce que ces personnes bénéficient d'une formation appropriée en matière de protection des données.

2.4. Mesures de sécurité des traitements

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles pour assurer la sécurité des données à caractère personnel. Ces mesures doivent garantir la protection des données contre toute violation de la sécurité entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Ces mesures incluent notamment :

- Le chiffrement des données à caractère personnel ;
- Les moyens permettant de rétablir la disponibilité et l'accès aux données à caractère personnel dans des délais appropriés en cas d'incident physique ou technique ;
- Des procédures régulières de test, d'analyse et d'évaluation de l'efficacité des mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité des traitements.

La modification des mesures techniques et organisationnelles déployées pour les traitements doit être autorisée préalablement par le Responsable de traitement, selon les modalités prévues à la clause 1.3.1. Quelle que soit la modification apportée, le Sous-traitant doit garantir un niveau de sécurité au moins équivalent entre les nouvelles mesures et les anciennes mesures.

2.5. Documentation et conformité

Le Sous-traitant s'engage à traiter rapidement et de manière adéquate les demandes du Responsable de traitement concernant les traitements des données, conformément aux présentes clauses.

Le Sous-traitant met à la disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du RGPD et/ou de la loi Informatique et libertés. À la demande du Responsable du traitement, le Sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité.

Le Responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du Sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.

Les parties mettent à la disposition de l'autorité de contrôle compétente, dès que celle-ci en fait la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

Le Sous-traitant doit être en mesure de fournir au Responsable de traitement à tout moment une liste des personnes autorisées à accéder aux données.

Le Sous-traitant doit communiquer sur demande la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence s'avère délicate dans le cadre d'architectures distribuées, il peut être demandé au prestataire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

2.6. Recours à des Sous-traitants ultérieurs

Le Sous-traitant dispose de l'autorisation générale du Responsable du traitement pour ce qui est du recrutement de Sous-traitants ultérieurs sur la base d'une liste convenue. Le Sous-traitant informe spécifiquement par écrit le Responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de Sous-traitants ultérieurs au moins trois (3) mois à l'avance, donnant ainsi au Responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des Sous-traitants ultérieurs concernés.

Le Sous-traitant fournit au Responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition ou, s'il préfère, de mettre un terme au contrat sans pénalité.

Lorsque le Sous-traitant recrute un Sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du Responsable du traitement), il le fait au moyen d'un contrat qui impose au Sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au Sous-traitant en vertu des présentes clauses. Le Sous-traitant veille à ce que le Sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

Le Sous-traitant demeure pleinement responsable, à l'égard du Responsable du traitement, de l'exécution des obligations du Sous-traitant ultérieur conformément au contrat conclu avec le Sous-traitant ultérieur. Le Sous-traitant informe le Responsable du traitement de tout manquement du Sous-traitant ultérieur à ses obligations contractuelles.

2.7. Transferts de données hors de l'Union européenne

Le Sous-traitant ne transfère pas de données à caractère personnel hors de l'Union européenne ni à des prestataires soumis à un droit extraterritorial tiers, sauf instruction écrite préalable du Responsable de traitement, ou si ce transfert est requis par la législation de l'Union ou d'un État membre auquel le Sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou à la loi Informatique et libertés. Dans ce cas, le Sous-traitant informe le Responsable de traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Le Sous-traitant doit fournir au Responsable de traitement une liste des pays destinataires mise à jour. En cas de modification des pays destinataires par le Sous-traitant, ce dernier doit en informer préalablement le Responsable de traitement.

Le Responsable de traitement convient que, lorsqu'un Sous-traitant recrute un Sous-traitant

ultérieur conformément à la clause 1.3.6 pour effectuer des activités de traitement pour son compte, et que ces activités impliquent un transfert de données à caractère personnel relevant du chapitre V du règlement (UE) 2016/679 ou soumettent le Sous-traitant ultérieur à une législation extraterritoriale, le Sous-traitant et le Sous-traitant ultérieur doivent garantir la conformité avec le chapitre V du règlement (UE) 2016/679 ou la loi Informatique et Libertés. Cette conformité peut être assurée par l'utilisation des clauses contractuelles types adoptées par la Commission en vertu de l'article 46, paragraphe 2, du règlement (UE) 2016/679, sous réserve que les conditions d'utilisation de ces clauses soient respectées et que les garanties exigées par le RGPD et la loi Informatique et Libertés soient préalablement validées par le délégué ministériel à la protection des données.

2.8. Sort des données

Aux termes du présent accord, le Sous-traitant s'engage à détruire toutes les données à caractère personnel traitées pour le compte du Responsable de traitement, de manière sécurisée et irréversible, sauf instruction contraire du Responsable de traitement.

2.9. Assistance au Responsable de traitement

2.9.1. Réponse aux demandes des personnes concernées

Le Sous-traitant transmet au Responsable du traitement dans les meilleurs délais et au plus tard vingt-quatre (24) heures après en avoir pris connaissance, de toute demande qu'il a reçue de la part de la personne concernée, à l'adresse suivante : dpiin-rssi@interieur.gouv.fr. Il ne donne pas lui-même suite à cette demande.

2.9.2. Notification des violations de données

Le Sous-traitant aide le Responsable de traitement à notifier toute violation de données à caractère personnel à l'autorité de contrôle compétente, ainsi qu'aux personnes concernées, conformément aux articles 33 et 34 du RGPD.

Le Sous-traitant notifie au Responsable du traitement dans les meilleurs délais et au plus tard vingt-quatre (24) heures après en avoir pris connaissance, toute violation de données à caractère personnel, à l'adresse suivante : dpiin-rssi@interieur.gouv.fr. Cette notification contient au moins :

- a)** une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;
- b)** les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
- c)** ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

2.9.3. Réalisation d'analyses d'impact

Le Sous-traitant assiste le Responsable de traitement dans la réalisation d'analyses d'impact relatives à la protection des données (AIPD) lorsque les traitements présentent un risque élevé

pour les droits et libertés des personnes concernées, conformément à l'article 35 du RGPD.

Le Sous-traitant fournit toutes les informations et ressources techniques nécessaires pour contribuer à la réalisation de l'AIPD.

2.9.4. Consultation préalable avec l'autorité de contrôle

Le Sous-traitant s'engage à fournir les informations nécessaires pour permettre au Responsable de traitement de consulter l'autorité de contrôle, conformément à l'article 36 du RGPD, lorsque l'analyse d'impact révèle un risque élevé non atténué par les mesures mises en place. Le Sous-traitant s'engage à collaborer pour ajuster les traitements afin de réduire les risques identifiés.

3. LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

Le Responsable de traitement s'engage à respecter les obligations légales qui lui incombent en vertu du Règlement (UE) 2016/679 et de la loi Informatique et Libertés.

Le Responsable de traitement s'engage à fournir au Sous-traitant les données nécessaires au traitement dans les conditions convenues. Il veille à ce que les données transmises soient exactes, complètes et mises à jour.

Le Responsable de traitement fournit des instructions documentées, précises et détaillées au Sous-traitant concernant le traitement des données à caractère personnel. Toute instruction supplémentaire ou modification doit être communiquée par écrit au Sous-traitant.

4. ANNEXE A : DESCRIPTION DU TRAITEMENT FRANCE IDENTITE

4.1. Catégories de personnes concernées dont les données à caractère personnel sont traitées :

Les usagers de l'application "France Identité", titulaires d'une carte nationale d'identité électronique (CNIE) française valide, utilisant un smartphone doté d'un système NFC compatible pour accéder aux fonctionnalités de l'application.

4.2. Catégories de données à caractère personnel traitées :

Données d'identité : nom, nom d'usage, prénom(s), date et lieu de naissance, nationalité, sexe, adresse postale, photographie extraite du composant électronique du titre.

Données d'identification du titre : numéro et type de carte d'identité, date de délivrance, date d'expiration, statut de validité (valide/invalidé/inconnu).

Données techniques : identifiant technique, historique des transactions (destinataire, statut, durée de validité des données transmises, horodatage des transactions).

4.3. Les données sensibles traitées et les limitations ou garanties appliquées :

Aucune donnée sensible n'est traitée au sens de l'article 9 du RGPD. Les mesures de sécurité comprennent la restriction stricte de l'accès aux données personnelles, réservée aux personnes habilitées, avec un registre des accès et une surveillance renforcée pour tout accès.

4.4. Nature du traitement :

Les données à caractère personnel sont exclusivement traitées pour l'identification et l'authentification des usagers auprès des services publics et privés via l'application France Identité. Cela inclut également la génération d'attestations électroniques d'attributs d'identités signées par l'État, permettant aux usagers de transmettre uniquement les attributs d'identité nécessaires dans le cadre de leurs démarches administratives ou privées.

4.5. Finalités pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable de traitement :

- Permettre aux usagers de s'authentifier en ligne de manière sécurisée via l'application France Identité.
- Générer des attestations électroniques d'attributs d'identité signées par l'État pour transmission à des tiers.
-

4.6. Durée du traitement :

Les données sont conservées pendant cinq (5) ans à compter de la dernière vérification d'identité ou jusqu'à la suppression du moyen d'identification électronique ou la désinstallation de l'application par l'utilisateur. Les données de l'historique des transactions sont conservées dans une limite déterminée par le responsable du traitement.

4.7. Traitement par les sous-traitants ultérieurs :

Aucun traitement par des sous-traitants ultérieurs n'est prévu dans ce cadre.

5. ANNEXE B : DESCRIPTION DU TRAITEMENT ATTESTATION FRANCE IDENTITE

5.1. Catégories de personnes concernées dont les données à caractère personnel sont traitées :

Les usagers de l'application "France Identité", notamment ceux qui souhaitent obtenir des attestations électroniques d'attributs. Ces attestations électroniques permettent aux usagers de France Identité de prouver certains attributs, comme leurs droits à conduire, auprès de tiers (administrations, autorités, services privés) sans divulguer l'intégralité de leurs données personnelles.

5.2. Catégories de données à caractère personnel traitées :

Données d'identification : nom, prénoms, date et lieu de naissance, sexe.

Données relatives aux droits à conduire : numéro de permis, date de délivrance, catégories de permis, validité, restrictions éventuelles.

Données relatives au certificat d'immatriculation des véhicules : Numéro d'immatriculation (plaque d'immatriculation), Informations administratives et techniques du véhicule, Marque et modèle, Type de véhicule, Résultat du contrôle technique.

5.3. Données sensibles traitées et limitations ou garanties appliquées :

Aucune donnée sensible n'est traitée au sens du RGPD. Des mesures de sécurité renforcées sont mises en place, incluant des restrictions d'accès strictes, la traçabilité des accès aux données et une surveillance accrue.

5.4. Nature du traitement :

Le traitement consiste à générer des attestations électroniques d'attributs, tels que le droit à conduire, à partir de données fournies par des Administrations partenaires.

5.5. Finalité pour laquelle les données à caractère personnel sont traitées pour le compte du responsable du traitement :

Permettre aux usagers de prouver leurs droits via des attestations électroniques, notamment lors de contrôles routiers ou dans d'autres démarches administratives. Une fois générées, ces attestations sont stockées localement sur l'application France Identité prouver certains attributs, comme leurs droits à conduire auprès de tiers.

5.6. Durée du traitement :

Les données ne sont conservées que pour la durée nécessaire à la génération de l'attestation électronique. Elles sont supprimées du serveur à l'issue du traitement.

5.7. Traitement par les sous-traitants (ultérieurs) :

Aucun traitement par des sous-traitants ultérieurs n'est prévu dans ce cadre.