RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API HERMES

(environnement de bac à sable)

Date de publication : 13/11/2023

FINANCES PUBLIQUES

Table des matières

1. Objet

Les présentes conditions générales d'utilisation ont pour objet de définir les conditions dans lesquelles les parties peuvent utiliser l'environnement de bac à sable de l'API HERMES de la Direction Générale des Finances Publiques (ci-après dénommé « DGFiP »).

L'API HERMES est une interface permettant l'échange de données entre la DGFiP et un partenaire conventionné.

Elle met ainsi à disposition un ensemble de données strictement utiles au partenaire conventionné dans le cadre de l'exercice de ses missions.

Le raccordement à l'API nécessite de manière cumulative :

- la saisie, par le partenaire conventionné, dans le formulaire de souscription en ligne « DataPass » du site internet api.gouv.fr, des données exactes et strictement nécessaires à la réalisation de la démarche ;
- la validation, par la DGFiP, des informations précisées dans le formulaire « DataPass » ;
- l'acceptation pleine et entière, ainsi que le respect des conditions générales d'utilisation telles que décrites ci-après.

Les données saisies dans le formulaire « DataPass » validé ainsi que l'acceptation des conditions générales d'utilisation valent convention entre la DGFiP et le partenaire conventionné.

2. Contexte et présentation du dispositif

2.1 Présentation du dispositif

L'API HERMES permet aux entités administratives (administration, ministère, organisme public, collectivité) et aux acteurs privés qui sont éligibles de déposer des biens en vue d'être vendus, d'avoir connaissance du statut de ces biens en cours de cession et préalablement déposés par un usager afin de permettre d'intégrer et de valider ces données dans leur système d'information. Elle permet également de prendre connaissance de certains éléments de référentiels nécessaires au dépôt de ces biens ou d'en compléter d'autres pour les mêmes raisons.

En effet, selon les dispositions de :

- l'article 98 de la loi n°2019-1428 du 24 décembre 2019 d'orientation des mobilités, l'ordonnance n°2020-773 et le décret n°2020-775 du 24 juin 2020 relatif aux fourrières automobiles, les dispositions du Code de la route sont modifiées afin de créer un système d'information national des fourrières en automobiles (SI fourrières) permettant l'échange d'informations entre les différentes autorités, dont le service du Domaine, intéressées à la procédure de mise en fourrière puis par la gestion du véhicule concerné ;

- des articles L325, L3258 et L325-9 du code de la route et du décret n°72-823 du 6 septembre 1972 fixant les conditions de remise à l'administration chargée des domaines des véhicules non retirés de fourrière par leurs propriétaires, les véhicules abandonnés en fourrière sont remis au domaine pour vente ;
- l'arrêté du 4 novembre 2020 relatif aux fourrières automobiles qui détaille les critères de remise au Domaine des véhicules abandonnés en fourrière.

Dans ces conditions, l'API HERMES permet d'enrichir les données de la DGFiP de biens destinés à être vendus, et restitue donc les données de la DGFiP en matière de statut des biens déposés et des éléments de référentiels utile au dépôt desdits biens conformément à l'obligation déclarative susvisée.

2.2 Rôle des acteurs intervenant dans le dispositif d'échange de données

2.2.1 Rôle du producteur d'API et qualité du fournisseur de données

Le producteur de l'API HERMES visée à l'article 2.1 est la DGFiP.

La finalité de l'API étant la mise à disposition ainsi que la modification d'information — incluant les opérations de création, de modification ou de suppression — (API dite de consultation et d'écriture), la DGFiP et le partenaire conventionné sont réputés être les fournisseurs de données (FD).

En l'espèce, le partenaire conventionné est le FD lorsqu'il s'agit de proposer un bien à la vente et la DGFiP est le FD lorsqu'il s'agit de restituer des informations sur les ventes.

2.2.2 Rôle du consommateur d'API et qualité du fournisseur de service

Le consommateur de l'API HERMES visée à l'article 2.1 est le partenaire conventionné. Il est réputé être le fournisseur de service (FS).

3. Conditions d'accessibilité au dispositif

La demande d'accès à l'API se réalise sur le site internet api.gouv.fr par le biais du formulaire dématérialisé « DataPass ». Elle nécessite la création d'un compte sur le site internet précité et le remplissage du formulaire de souscription en ligne. Les présentes conditions générales d'utilisation n'ont pas vocation à couvrir l'utilisation dudit site internet.

3.1 Conditions juridiques

3.1.1 Conditions générales

L'accès au dispositif API est soumis à deux conditions cumulatives :

- Le consommateur de l'API sollicitant le raccordement au dispositif doit être autorisé à demander et exploiter les données échangées par API dans le cadre de l'exercice de ses missions.
- Le périmètre des informations sollicitées par le consommateur de l'API doit être strictement nécessaire à l'exercice de la mission pour laquelle il demande les données et se justifier par des dispositions législatives ou réglementaires, ou par une délibération d'une collectivité locale, le cas échéant.

À ce titre, le consommateur de l'API devra communiquer dans le cadre de la procédure de raccordement le ou les textes législatifs ou réglementaires justifiant son accès aux données. Le producteur de l'API opérera une analyse juridique systématique afin de déterminer si le partenaire conventionné est habilité à connaître ces données dans le cadre de ses missions.

En outre, le consommateur de l'API devra fournir au producteur de l'API :

- La description de sa démarche et de l'usage qui sera fait des données
- Le périmètre des informations visées par la demande
- Le ou les services destinataires de ces données

3.1.2 Conditions spécifiques à l'environnement de bac à sable

Les données que le producteur de l'API met à disposition sont des données fictives et ne rentrent pas dans le cadre des données à caractère personnel.

Le consommateur de l'API, s'il agit en tant que fournisseur de données, devra s'assurer que les données transmises à l'API sont des données fictives, expurgées de tout élément pouvant être considéré comme une donnée à caractère personnel.

L'accès de l'API en environnement de bac à sable n'est pas conditionné aux vérifications de sécurité définis dans les CGU des environnements de production. Ces éléments sont fournis pour information et dans le but de faciliter les démarches ultérieures en annexe des présentes CGU. Cependant il se doit de respecter les engagements de sécurité détaillés en section 8.

Le consommateur de l'API s'engage à réaliser une recette fonctionnelle dont il soumettra les résultats au producteur de l'API lors de la demande de raccordement à l'API en environnement de production.

Enfin, le consommateur de l'API devra communiquer, lors de la souscription à l'environnement de bac à sable le ou les textes législatifs ou réglementaires justifiant de l'accès aux données par le biais du formulaire « DataPass ».

3.2 Déclaration de conformité des traitements à la réglementation relative à la protection des données à caractère personnel

Le consommateur de l'API n'est soumis à aucune obligation déclarative concernant les données à caractère personnel dans le cadre de l'environnement de bac à sable.

Toutefois, il est porté à sa connaissance que, dans le cadre des CGU des environnements de production, il devra, en amont du raccordement, déclarer au producteur de l'API l'accomplissement des formalités en matière de protection des données à caractère personnel, en cochant la case à cet effet dans le formulaire « DataPass » lors de la souscription à l'environnement de production.

4. Description du dispositif de transmission des données

En fonction du cadre juridique et des contrats d'interfaces publiés, le consommateur de l'API peut interroger l'API à partir des paramètres suivants :

- l'identifiant du bien sous la forme d'un nombre
- une période donnée (date de début et date de fin) afin de récupérer un ensemble de biens

Le producteur de l'API, procède à une série de contrôles en amont de la consultation ou de la modification des données visant à limiter l'accès aux seules données autorisées pour le consommateur de l'API concerné au regard du périmètre et des textes juridiques précisés dans sa demande de raccordement :

- la validité du certificat du consommateur de l'API (un certificat SSL authentifiant le demandeur et garantissant la sécurisation du transfert des données) ;
- l'adresse IP de l'appelant ;
- la présence et la conformité de l'identifiant technique de l'appelant ;
- l'identité du consommateur de l'API ;
- les droits du consommateur de l'API sur les données demandées ou transmises pour la période concernée.

Une fois ces contrôles effectués, les données conformes à la contractualisation entre le consommateur de l'API et le producteur de l'API pourront être restituées ou envoyées.

Les données transmises par le producteur de l'API devront être stockées dans un silo sécurisé du consommateur de l'API permettant de garantir leur intégrité.

En revanche, si les vérifications opérées par le producteur de l'API ne sont pas conformes à la contractualisation, aucune donnée ne fera l'objet d'un échange.

L'accès à l'API s'effectue via la plateforme d'API Management (ci-après dénommé APIM) qui opère la gestion des API de la DGFiP. L'APIM offre aux partenaires conventionnés des API DGFiP des environnements de test (appelés « bac à sable ») et de production pour toutes les API et sécurise les appels effectués.

Un compte d'accès à cette plateforme sera généré et les moyens d'accès seront notifiés au responsable technique mentionné dans le formulaire de souscription « DataPass ».

5. Les engagements des parties

5.1 Obligations du producteur de l'API

Au titre de producteur d'API, la DGFiP est chargée d'instruire chaque demande de raccordement à l'API pour vérifier que ladite demande est éligible au dispositif. Elle doit notamment apprécier le caractère nécessaire des données au regard des conditions prévues par le texte législatif ou réglementaire régissant la procédure en cause.

La durée de conservation des données de l'échange (identification de l'usager qui fait l'objet de la demande, identification du consommateur de l'API, données échangées…) est limitée et justifiée au regard du besoin pour lequel elles sont collectées.

Par ailleurs, le producteur de l'API s'engage à fournir aux consommateurs de l'API toute information utile et nécessaire en cas d'événement de sécurité susceptible d'affecter notamment l'échange de données ou les données elles-mêmes et ce, dans les meilleurs délais.

5.2 Obligations du consommateur de l'API

Il incombe au consommateur de l'API de s'assurer de/du :

- respect de la réglementation relative à la protection des données à caractère personnel ;
- la validité et de la mise à jour le cas échéant, des données de contact du responsable de traitement déclarées dans le « DataPass » ;
- traitement des données échangées pour la seule et unique finalité déclarée par le biais du « DataPass » ;
- la mise à disposition en amont de l'échange de données, de l'affichage à l'usager du périmètre et de l'origine des données échangées avec le producteur de l'API sous une forme littérale pour l'informer explicitement du dispositif d'échange de données pour la démarche envisagée et de l'ensemble des informations requises par la réglementation relative à la protection des données à caractère personnel ;
- l'accès aux données échangées aux seuls agents des services compétents ou personnels habilités pour instruire les demandes des usagers. Le ou les services destinataires des données devront être expressément communiqués au producteur de l'API par le biais du « DataPass » ;
- la mise en œuvre de toutes les mesures techniques et organisationnelles nécessaires pour garantir l'intégrité, la confidentialité et la sécurité des données échangées incluant la mise en œuvre d'un dispositif de traçabilité ;
- l'absence de stockage des identifiants au-delà du temps nécessaire au traitement de la demande de l'usager, sauf cadre juridique l'y autorisant.

Il appartient au consommateur de l'API d'informer par écrit ses partenaires en cas de délégations de service ou recours à des contrats de sous-traitance dans le cadre de la

mise en place du service ou de l'application utilisant les données échangées. Cette information doit intervenir dans un délai raisonnable avant la mise en œuvre de la délégation de service ou la sous-traitance.

Le consommateur de l'API devra également fournir par écrit au producteur de l'API toute information utile et nécessaire en cas d'événement de sécurité susceptible notamment d'affecter la transmission des données ou les données elles-mêmes et ce, dans les meilleurs délais.

5.3 Obligations du fournisseur de données

Dès qu'ils agissent en tant que fournisseurs de données, tel que défini à l'article 2.2.1, la DGFiP et le partenaire conventionné s'engagent à transmettre, pour l'usager concerné, les seules données autorisées pour le cas d'usage concerné selon les modalités décrites dans la documentation fonctionnelle et technique de l'API (publiée sur le « Store » APIM de la DGFiP).

Dans le cas où le fournisseur de données traite des données à caractère personnel, il est soumis aux obligations de respect des règles définies dans la section 6.

6. Protection des données à caractère personnel

6.1 Traitements de données à caractère personnel opérés dans le cadre de l'échange de données

Dans le cadre de l'échange de données par le biais de l'API, la DGFiP et le partenaire conventionné peuvent opérer des traitements de données à caractère personnel.

À ce titre, chacun agit en sa qualité de responsable de traitement pour les finalités qui leur sont propres.

Chaque responsable de traitement s'engage ainsi à effectuer les opérations de traitements de données à caractère personnel à l'occasion du présent dispositif d'échange de données en conformité avec les dispositions du Règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après dénommées la réglementation).

6.2 Confidentialité

Les responsables de traitement doivent veiller à ce que les personnes autorisées à traiter les données à caractère personnel soient soumises à une obligation appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

Les responsables de traitement veillent à ce que les agents ou personnels habilités à

consulter les données restituées par le fournisseur de données n'aient accès qu'aux données strictement nécessaires à l'exercice de leurs missions.

6.3 Relations vis-à-vis des personnes physiques concernées

Il incombe à chaque responsable de traitement de porter à la connaissance des personnes physiques concernées par le traitement de leurs données à caractère personnel, les informations prévues par la réglementation relative à la protection des données à caractère personnel et notamment les articles 13 et 14 du Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dans les conditions et modalités prévues par ces mêmes articles.

Aussi, les personnes physiques dont les données à caractère personnel sont traitées peuvent exercer les droits que la réglementation leur confère à l'égard de chacun des responsables de traitement par le biais de leur point de contact respectif.

Il appartient à chacun des responsables de traitement d'assurer respectivement la prise en charge de l'exercice de ces droits par les personnes physiques concernées.

6.4 Coopération

Les responsables de traitement s'engagent de manière générale à une coopération réciproque et loyale pour la bonne exécution du dispositif d'échange de données et le traitement licite des données à caractère personnel qui en découle.

Sur demande écrite, chacun des responsables de traitement peut se faire se communiquer par l'autre responsable de traitement toute information utile nécessaire pour la bonne exécution de leurs obligations respectives en matière de protection des données à caractère personnel.

6.5 Sous-traitants

Dans l'hypothèse d'un recours à un ou plusieurs sous-traitants directs ou indirects par les responsables de traitement, ceux-ci devront s'engager à faire respecter par toute personne agissant pour leur compte et ayant accès aux données à caractère personnel traitées dans le cadre du présent téléservice, les mêmes obligations en matière de protection des données à caractère personnel que celles fixées par le présent article en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées permettant d'assurer que tout traitement de données à caractère personnel répond aux exigences de la réglementation en matière de protection des données à caractère personnel.

Les responsables de traitement s'engagent chacun pour ce qui les concerne pleinement et demeurent responsables du respect, par leurs sous-traitants, des obligations de protection des données à caractère personnel et de respect des règles de confidentialité et de secret professionnel prévues aux présentes CGU.

6.6 Violation de données à caractère personnel

Les responsables de traitement s'engagent, chacun pour ce qui les concerne, à notifier à la Commission Nationale de l'Informatique et des Libertés (CNIL) toute violation de données à caractère personnel à risque pour les droits et libertés des personnes concernées dans le cadre du dispositif d'échange de données dans les soixante-douze (72) heures au plus tard après en avoir pris connaissance, dès lors que ces données à caractère personnel ne sont couvertes par aucun procédé d'anonymisation irréversible.

Les responsables de traitement sont tenus, chacun pour ce qui les concerne, à notifier dans les meilleurs délais, les violations de données à caractère personnel aux personnes physiques concernées lorsque ces violations sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées.

Par ailleurs, en cas de violation de données à caractère personnel ayant un impact sur le dispositif d'échanges de données par API, chaque responsable de traitement s'engage à informer les autres responsables de traitement de ladite violation accompagnées le cas échéant, de toute documentation utile.

6.7 Responsabilité

Conformément aux dispositions de la réglementation en matière de protection des données à caractère personnel, toute personne physique ayant subi un dommage matériel ou moral du fait d'une violation des dispositions précitées a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Il est convenu que chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage subi par la personne physique concernée à hauteur respective de leur part de responsabilité dans celui-ci.

6.8 Traitements de données opérés dans le cadre de la mise à disposition de l'API

La DGFiP traite les données à caractère personnel collectées :

- dans le formulaire de souscription « DataPass » du site internet api.gouv.fr
- dans le cadre de l'utilisation des API par les partenaires conventionnés (notamment par les journaux générés par les systèmes d'information ou toutes autres traces de connexion et d'utilisation) et les échanges subséquents avec ces partenaires.

Ce traitement a pour finalité la mise en place et la gestion opérationnelle des échanges de données réalisées par le biais des API mis à disposition des partenaires habilités par la DGFiP. Il est mis en œuvre dans le cadre des missions d'intérêt public de la DGFiP et de ses obligations légales au titre des dispositions du Code des relations entre le public et l'administration ou de tout autre source réglementaire spécifique à ce sujet.

Les données collectées dans le cadre de la souscription du « DataPass » sont conservées pendant six (6) ans à compter de l'arrêt de la délivrance des données par voie d'API au

demandeur.

Les concepteurs et administrateurs des API au sein de la DGFiP sont les seuls destinataires de ces données.

Les personnes concernées (acteurs intervenant dans le cadre de la souscription au « DataPass » : demandeur, responsable de traitement et responsable technique) peuvent accéder aux données les concernant, les rectifier, demander leur effacement ou exercer leurs droits à la limitation du traitement de leurs données en contactant l'adresse :

dtnum.donnees.demande-acces@dgfip.finances.gouv.fr

Si ces personnes, après avoir contacté la DGFiP, estiment que leurs droits ne sont pas respectés, elles peuvent adresser une réclamation à la CNIL.

7. Coût du service

Aucune contrepartie financière directe n'est demandée par l'une ou l'autre des parties dans le cadre des échanges de données proposés par l'API HERMES.

8. Sécurité

Dans le cadre des dispositions légales et réglementaires en matière de protection du secret et des données à caractère personnel, le consommateur de l'API et le producteur de l'API s'engagent à prendre toutes les mesures utiles et nécessaires pour assurer la protection absolue des données ou supports protégés qui peuvent être détenus ou échangés par les parties.

Un engagement particulier doit être pris sur les points suivants :

- les spécifications de sécurité du protocole OAuth2.0[1] doivent être respectées dans l'implémentation des différentes briques du dispositif ;
- l'engagement du consommateur de l'API en matière de sécurité doit s'appuyer sur une analyse de risques et des audits de sécurité réguliers prenant en compte les spécifications du protocole OAuth2.0 précité ;
- les parties doivent s'engager à couvrir les risques portant sur leurs systèmes d'information et corriger les vulnérabilités détectées ; en cas de vulnérabilité majeure, la partie concernée s'engage à ne pas mettre la brique applicative en production ;
- les parties doivent s'engager à mettre en œuvre des systèmes de détection d'événements de sécurité et à opérer une surveillance organisée de ces événements de sécurité ;

1 https://tools.ietf.org/html/rfc6749

- les engagements en termes de sécurité des différentes parties pourront être vérifiés par l'ANSSI ; les livrables des audits et le suivi de ces audits doivent être fournis sur sa demande.

Les différentes parties s'engagent par ailleurs à mettre en place un processus de gestion des incidents de sécurité, avec les phases suivantes :

- Mesures de réponses immédiates : notamment l'isolation ou la coupure du service
- Investigations :
    - rassemblement et préservation de toutes les informations disponibles pour permettre les investigations, notamment obtention des journaux couvrant la période d'investigation ;
    - détermination du périmètre ;
    - qualification de l'incident, identification du fait générateur et analyse d'impact.
- Traitement :
    - si nécessaire, activation d'une cellule de crise ;
    - restrictions temporaires d'accès ;
    - actions d'alerte (RSSI) réciproques et de communication.
- Après résolution de l'incident :
    - analyse de l'incident de sécurité pour détermination de la cause et corrections associées ;
    - vérification avant remise en service que l'élément malveillant a été supprimé et que les éventuelles vulnérabilités sont corrigées ;
- Éventuelles suites judiciaires (dépôt de plainte).

La mise en œuvre d'un tel processus implique au préalable :

- la mise en place de dispositifs permettant la détection d'intrusions, la corrélation d'événements de sécurité, la surveillance des systèmes d'information (notamment la détection de comportements anormaux) incluant un système de traçabilité des accès et actions des utilisateurs y compris ceux automatisés par robot ou traitement par lots, sur les données et processus ;
- une revue des incidents faite régulièrement pour quantifier et surveiller les différents types d'incidents ;
- la mise en place d'une politique de journalisation ;
- la définition des acteurs (tels que les utilisateurs ou les exploitants), des circuits d'alerte, la sensibilisation de ces acteurs ;
- des tests des processus d'alerte.

9. Gestion des mises en production

9.1 Identification des points de contact

9.1.1 Contact DGFiP pour l'assistance technique et fonctionnelle

Une boîte aux lettres fonctionnelle est mise à disposition pour toute question d'assistance technique et fonctionnelle :

apimanagement.support@dgfip.finances.gouv.fr

9.1.2 Contact DGFiP pour la souscription au « DataPass »

Pour toute question liée à la demande de souscription « DataPass » à l'API, une boîte aux lettres fonctionnelle est mise à disposition :

dtnum.donnees.demande-acces@dgfip.finances.gouv.fr

9.1.3 Contact du fournisseur de service

Le consommateur de l'API, en tant que fournisseur de service vis-à-vis de ses usagers, précise les contacts à privilégier dans le cadre de sa demande de raccordement à l'API formulée sur le formulaire « DataPass ».

9.2 Volumétrie

Par défaut, le quota d'appels de l'API est fixé à 50 appels par minute.

9.3 Suivi des mises en production

Il n'y a pas d'outil partagé entre les partenaires sur le suivi des mises en production. Ce partage est assuré obligatoirement par une communication écrite par courriel. L'usage du téléphone entre les parties pour la programmation des mises en production est à réserver aux situations d'urgence. Les changements doivent être annoncés quatorze (14) jours ouvrés avant leur application en conditions nominales et sept (7) jours ouvrés avant leur application en conditions d'urgence.

Les deux parties s'engagent à ne pas communiquer aux usagers les points de contact décrits dans le présent document.

10. Les critères DICP

Le bureau architecture et norme (Bureau SI1) de la DGFiP a défini une méthode d'intégration de la sécurité dans les projets (démarche ISP).

Cette démarche comporte notamment une phase de sensibilisation globale de la sécurité du projet qui permet aux acteurs métiers de mesurer la sensibilité globale du projet en termes de disponibilité, intégrité, confidentialité, preuve et contrôle (DICP).

La sensibilité du projet (SGP) sur le périmètre d'analyse est alors évaluée à l'aide des critères de sécurité fournis en annexe de ces CGU et se traduit par un unique profil DICP. Ce profil correspond à l'évaluation des niveaux de service de la sécurité qu'il requiert pour chacun de ces critères.

S'agissant du projet API HERMES dans la mise en œuvre par le producteur de l'API, le profil DICP est le suivant :

D	I	C	P
3 (24h)	3	4	3

11. Qualité du service

Le niveau de disponibilité est dit "fort" au sens DGFiP. Ainsi, les exigences pour ce niveau de disponibilité sont les suivantes :

- API : ouverture toute l'année ;
- Périodes sensibles identifiées : Périodes d'activités du domaine professionnel ;
- Plages d'ouverture du service : 0:00-24:00, 7j/7 (service non disponible pour maintenance sur une plage de 2 heures entre 23:00 et 6:00) ;
- Offre de couverture de service de la DGFiP : 7:00-20:00 ;
- L'offre de couverture de service et le taux de disponibilité du téléservice est précisé par le consommateur de l'API lors de sa demande de raccordement à l'API.

La mesure du taux de disponibilité se fait sur la plage d'ouverture du service, que les indisponibilités soient programmées ou non.

- Pas de besoin d'astreintes les soirs et les week-ends ;
- Garantie du temps de rétablissement en cas d'incident estimé à 24 heures ouvrées (une fois par trimestre) ;
- Perte maximale de données tolérable estimée à 24 heures ;
- Taux de disponibilité des plages de couverture : 97,16 %.

12. Suspension, modification et évolution du service

Le producteur de l'API se réserve la liberté de faire évoluer, de modifier ou de suspendre, sans préavis, le service pour des raisons de maintenance, de sécurité ou pour tout autre motif jugé nécessaire.

En pareille hypothèse, le consommateur de l'API en sera dûment averti par écrit et dans les meilleurs délais.

13. Durée de validité des conditions générales d'utilisation

Les présentes conditions générales d'utilisation entrent en vigueur dès leur acceptation et demeurent applicables pendant toute la durée de l'échange de données et ce, jusqu'à son terme.

14. Modification des conditions générales d'utilisation et modalités de résiliation

Les termes des présentes CGU peuvent être modifiées ou complétées à tout moment, sans préavis, en fonction des modifications apportées au service, de l'évolution de la législation ou pour tout autre motif jugé nécessaire.

Toute modification des CGU fera l'objet d'une information auprès de la partie impactée.

En cas de nullité d'une ou plusieurs des clauses des présentes CGU en application d'une loi, d'un règlement ou à la suite d'une décision définitive rendue par une juridiction compétente, les autres clauses des CGU conserveraient leur force obligatoire dans la limite de ladite décision.

Par ailleurs, si l'une des parties souhaite mettre fin à l'échange de données avec l'API, elle en informe l'autre partie par écrit, en indiquant les motifs de sa décision.
Un préavis de deux mois est alors nécessaire avant que la résiliation ne soit pleinement effective. Durant cette période, l'échange de données via l'API est maintenu conformément aux présentes CGU.

Cette disposition ne couvre pas le cas particulier d'une situation où un problème de sécurité chez l'une des parties serait détecté.

15. Loi applicable et litiges

La DGFiP ne peut être tenue responsable des pertes et/ou préjudices, de quelque nature qu'ils soient, qui pourraient être causés à la suite d'un dysfonctionnement ou d'une indisponibilité du service. De telles situations n'ouvriront droit à aucune compensation financière.

Aucune des parties ne peut être tenue pour responsable de toute inexécution ou retard dans l'exécution de ses obligations par suite d'évènements échappant au contrôle raisonnable d'une partie, tels que les attaques par déni de service, la défaillance d'un hébergeur ou d'un fournisseur d'accès ou de service, les grèves, les pénuries, les émeutes, les incendies, les cas de force majeure, les catastrophes naturelles, la guerre et le terrorisme.

Les présentes CGU et tous les différends qui en découlent ou qui s'y rapportent, seront régis exclusivement par la loi française.

Les tribunaux français auront compétence exclusive pour trancher tout différent découlant des CGU, de leur interprétation ou application.

Chaque partie reconnaît la compétence exclusive de ces tribunaux et s'y soumet.

Glossaire	
APIM	API Management (plateforme de gestion des API de la DGFiP)
Bac à sable	Environnement de test (exploitant des données fictives)
CGU	Conditions générales d'utilisation
DataPass	Formulaire de souscription pour l'habilitation juridique d'accès aux données restreintes
DGFiP	Direction Générale des Finances Publiques
DTNum	Délégation à la transformation numérique
FD	Fournisseur de données (tel que défini à l'article 2.2.1)
FS	Fournisseur de services (dans le cas présent, le partenaire conventionné)
Production	Environnement de production (exploitant des données réelles)
Responsable de traitement	Personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement
RGPD	Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
RGS	Référentiel général de sécurité
RSSI	Responsable de la Sécurité des Systèmes d'Information

Annexes

Tableaux des critères DICP

Niveau de service	1 Élémentaire	2 Important	3 Fort	4 Stratégique
DISPONIBILITE	**D1** Interruption acceptable au delà de 5 jours. **Pas de remise en cause des services essentiels du SI.** Interruption =] 5 jours ; 15 jours]	**D2** La fonction ou le service ne doit pas être interrompu plus de 5 jours. **Les conséquences sur les services essentiels du SI sont importantes.** Interruption =] 48 heures ; 5 jours]	**D 3** La fonction ou le service ne doit pas être interrompu plus de 48 heures. **Les conséquences sur les services essentiels du SI sont graves.** Interruption =] 4 heures ; 48 heures]	**D4** Le service doit toujours être fourni. **Haute disponibilité requise.** [0 ; 4 heures]
INTEGRITE	**I 1** Atteinte à l'intégrité des fonctions ou informations manipulées, **acceptée si détectée et signalée.**	**I 2** Atteinte à l'intégrité des fonctions ou informations manipulées, **tolérée si détectée, signalée et corrigée dans un délai raisonnable.**	**I 3** Atteinte à l'intégrité des fonctions ou informations manipulées, **tolérée si arrêt immédiat des opérations jusqu'au rétablissement de l'intégrité.** Garantie constante de l'intégrité des fonctions ou informations manipulées.	**I 4** Atteinte à l'intégrité des fonctions ou informations manipulées, **inacceptable.** Les fonctions et informations doivent être toujours intègres.
CONFIDENTIALITE	**C 1** Informations pouvant être communiquées à tout public.	**C 2** Informations nécessitant une diffusion restreinte aux acteurs de la **DGFIP**.	**C 3** Informations accessibles uniquement à des populations **identifiées, authentifiées et habilitées**.	**C 4** Informations accessibles uniquement à des personnes habilitées et authentifiées de manière forte au travers de dispositifs de sécurité **renforcés**.
PREUVE ET CONTROLE	**P 1** Éléments de preuve non nécessaire.	**P 2** Éléments de preuve**nécessaires avec mise à disposition dans un délai raisonnable**. Exploitation de logs « techniques » traduisant un niveau de trace « simple ».	**P 3** Éléments de preuve**nécessaires avec mise à disposition rapide.** Exploitation de traces dites « fonctionnelles » ou « métier » traduisant un niveau de trace "détaillée".	**P 4** Éléments de preuve **indispensables permettant d'apporter des éléments sur la réalisation d'une opération par un acteur extérieur à la DGFIP.**

Engagements de sécurité pour les environnements de production

Note : Cette section reprend les CGU de production relatives aux engagements de sécurité du consommateur de l'API lorsqu'il demande un accès sur les environnements de production. Elles sont reprises à des fins d'information du consommateur de l'API afin qu'il puisse en tenir compte et lui offrir la possibilité d'anticiper les actions nécessaires pour y répondre. De ce fait, les éléments qui sont décrits dans cette annexe n'engagent pas le consommateur de l'API vis-à-vis de l'environnement de bac à sable, objet des présentes CGU.

Engagements concernant le niveau de sécurité

Le consommateur de l'API doit attester formellement du niveau de sécurité du service qu'il opère auprès de la DGFiP.

Cela peut prendre la forme :

1. pour les autorités administratives auxquels le Référentiel général de sécurité (RGS) s'applique, d'une attestation d'homologation de sécurité ;
2. pour les consommateurs de l'API ne relevant pas du champ d'application du RGS, de la fourniture d'un questionnaire de sécurité renseigné selon le modèle fourni par la DGFiP.

Homologation de sécurité

L'homologation de sécurité du consommateur de l'API doit être prononcée avant l'effectivité des échanges en production.

L'attestation d'homologation est demandée par le producteur de l'API avant toute mise en production.

Lorsque l'homologation de sécurité comporte des réserves, ou prend la forme d'une autorisation provisoire d'emploi, un échange est réalisé entre le consommateur de l'API et le producteur de l'API afin d'expliciter les réserves, et permettre de valider l'ouverture des échanges en production.

Le consommateur de l'API s'engage à communiquer une nouvelle attestation d'homologation de sécurité trois (3) mois avant la fin de la période de validité de l'homologation de sécurité actuelle ou de l'autorisation provisoire d'emploi si celui-ci souhaite encore bénéficier du raccordement. En l'absence d'une telle transmission, l'échange de données sera suspendu jusqu'à ce que le consommateur de l'API communique ce document au producteur de l'API.

Enfin, le consommateur de l'API s'engage à informer le producteur de l'API lorsque les évolutions de risque qu'il identifie dans son processus courant de suivi des homologations font apparaître le besoin d'une nouvelle homologation, ainsi qu'à communiquer une nouvelle attestation d'homologation dès que possible.

Questionnaire de sécurité

Dans cette procédure, le producteur de l'API transmet au consommateur de l'API un modèle de questionnaire de sécurité qu'il complète en parfaite transparence et le lui retourne dans le cadre du processus de souscription.

Ce questionnaire répond à deux groupes d'interrogations :

- un premier groupe, qui permet de prendre de manière directe une décision d'ouverture ou de refus d'ouverture des échanges en production.
- un deuxième groupe, qui fait l'objet d'une analyse approfondie par la DGFiP, et qui peut conduire celle-ci à émettre des préconisations de renforcement ou d'ajustement du dispositif opérationnel ou de sécurité du consommateur de l'API. Ce dernier s'engage par principe dès la souscription à les examiner et à planifier leur réalisation.

Dans l'hypothèse où l'analyse approfondie des réponses du consommateur de l'API ferait apparaître un risque critique pour les données de la DGFiP, une résolution sous contrainte de délai peut être demandée au consommateur de l'API, voire une décision de coupure préemptive peut être prise ; décision dont serait informé le consommateur de l'API.

De la même manière qu'une homologation a une durée limitée de validité, afin de rendre récurrent le contrôle de la cohérence entre les risques et les mesures prises, **le questionnaire de sécurité devra être mis à jour régulièrement, au plus, tous les trois ans par le consommateur de l'API, et adressé au producteur de l'API.**