RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API R2P

(environnement de production)

Date de publication : [20/08/2022]

FINANCES PUBLIQUES

Historique des versions		
Date	**Version**	**Objet**
25/09/2020	v2.5	Publication sur api.gouv.fr
20/08/2022	**V3.0**	**Modification - Publication sur api.gouv.fr**

Glossaire	
APIM	API Management (plateforme de gestion des API de la DGFiP)
Bac à sable	Environnement de test (données fictives)
CGU	Conditions générales d'utilisation
Data Pass	Formulaire de souscription
DGFiP	Direction Générale des Finances Publiques
DTNum	Délégation à la transformation numérique
FD	Fournisseur de données (au cas présent, la DGFiP)
FS	Fournisseur de services (au cas présent, le partenaire)
Production	Environnement de production (données réelles)
R2P	Recherche de personnes physiques
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel général de sécurité
RSSI	Responsable de la Sécurité des Systèmes d'Information

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 production de l'API R2P (Recherche de personnes physiques) de la Direction Générale des Finances Publiques (ci-après dénommée « DGFiP »).

L'API R2P est une interface permettant l'échange de données d'un usager entre la DGFiP et un partenaire conventionné.

Elle met ainsi à disposition certaines données d'identification des personnes physiques 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 « Data Pass », des données exactes et strictement nécessaires à la réalisation de la démarche ;
- la validation, par la DGFiP, des informations précisées dans le formulaire de souscription en ligne « Data Pass » du site api.gouv.fr ;
- 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 « Data Pass » 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 R2P fait appel aux différents référentiels nationaux de la DGFiP afin de rechercher et de restituer des éléments relatifs à l'état civil et l'adresse d'un usager ; éléments fiables dont les états civils sont, pour une grande majorité, certifiés par l'INSEE (+99%) et les adresses conformes aux normes topographiques nationales.

La transmission de données par le biais de ce dispositif doit se fonder sur un cadre légal permettant d'accéder aux données de la DGFiP.

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

2.2.1 Rôle du fournisseur de données (FD)

Le fournisseur de données est chargé de transmettre un ensemble d'informations à un fournisseur de service dûment habilité sous réserve de la nécessité d'accéder auxdites informations, justifiée par un texte législatif ou réglementaire.

Dans le cadre de l'accès à l'API R2P, la DGFiP est le fournisseur de données.

2.2.2 Rôle du fournisseur de service (FS)

Le partenaire conventionné qui sollicite le raccordement à l'API R2P dans le cadre de ses obligations légales et réglementaires pour des missions d'intérêt général est le fournisseur de service.

3. Conditions d'accessibilité au dispositif

La demande d'accès à l'API R2P se réalise sur le site www.api.gouv.fr par le biais du formulaire « Data Pass ». 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

Le fournisseur de service sollicitant le fournisseur de données doit être autorisé à demander et exploiter les données dans le cadre de l'instruction de démarches administratives ou du respect d'une ou plusieurs obligations légales qui lui incombent.

Aussi, celui-ci doit fonder sa demande d'accès aux données sur une dérogation au secret professionnel autorisant la DGFiP à lui communiquer des informations (par exemple les articles L.114-8 et R.114-9-4 du code des relations entre le public et l'administration).

Le périmètre des informations sollicitées par le fournisseur de service doit être justifié par des dispositions législatives ou réglementaires ou, le cas échéant, par une délibération d'une collectivité locale. Il doit être strictement nécessaire à l'exercice de la mission pour laquelle les données sont demandées.

La communication, à la DGFiP, du(des) texte(s) juridique(s) permettant de justifier l'accès aux données doit intervenir au plus tard lors de la souscription à l'environnement de production par le biais du formulaire « Data Pass » en ligne.

Outre le cadre juridique, le périmètre, la démarche concernée/l'usage des données, le quota/la volumétrie des appels, le(s) service(s) destinataire(s) des données, l'attestation d'homologation de sécurité ou son équivalent pour les entités n'entrant pas dans le périmètre d'application du Référentiel général de sécurité (Cf § 3.3), ainsi que la confirmation d'une recette fonctionnelle doivent être également communiqués au fournisseur de données.

De plus, des pièces justificatives supplémentaires doivent être également transmises au fournisseur de données selon la nature des relations entre les acteurs intervenant dans le cadre de la souscription au « Data Pass » (demandeur, responsable de traitement et responsable technique).

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

Le fournisseur de service doit, en amont du raccordement, déclarer au fournisseur de données s'être assuré de la conformité des traitements à la réglementation relative à la protection des données à caractère personnel, en cochant la case à cet effet dans le formulaire en ligne « Data Pass » lors de la souscription à l'environnement de production. **Cette déclaration engage la responsabilité du fournisseur de service.**

3.3 Engagement concernant le niveau de sécurité

Le fournisseur de service 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 fournisseurs de service 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.

À titre transitoire, les fournisseurs de services relevant du RGS pourront utiliser la procédure prévue au 2) ci-dessus.

3.3.1 Homologation de sécurité

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

L'attestation d'homologation est demandée par le fournisseur de données avant toute mise en production.

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

Le fournisseur de service s'engage à communiquer une nouvelle attestation d'homologation de sécurité 3 mois avant la fin de cette durée 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 fournisseur de service communique ce document au fournisseur de données.

Enfin, le fournisseur de service s'engage à informer la DGFiP 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.

3.3.2 Questionnaire de sécurité

La DGFiP transmet au fournisseur de service un modèle de questionnaire de sécurité qu'il complète en parfaite transparence et retourne à la DGFiP dans le cadre du processus de souscription.

Ce questionnaire adresse 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 fournisseur de service. 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 fournisseur de service ferait apparaître un risque critique pour les données de la DGFiP, une résolution sous contrainte de délai peut être demandée au fournisseur de service, voire une décision de coupure préemptive peut être prise ; décision dont serait informé le fournisseur de services.

De la même manière qu'une homologation à 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 fournisseur de service, et adressé à la DGFiP**.

4. Description du dispositif de transmission des données

En fonction du cadre juridique, le fournisseur de service peut interroger le fournisseur de données à partir de/du :

- l'état civil complet (nom, prénom, date et lieu de naissance) ;
- l'état civil dégradé et des éléments d'adresse (les noms et prénoms doivent alors être impérativement renseignés, de même que les éléments suivants : code pays, code département et code commune de l'adresse. Les autres éléments d'état civil (date et lieu de naissance) et les autres éléments d'adresse (libellé voie, numéro de voirie et indice de répétition) peuvent être renseignés de manière facultative) ;
- SPI ou NFP (identifiant fiscal ou « numéro SPI »).

Les deux derniers modes d'interrogation sont possibles uniquement dans le cadre du décret n° 2022-814 du 16 mai 2022 relatif aux conditions dans lesquelles les collectivités territoriales, les établissements publics qui leur sont rattachés et les établissements publics sociaux et médico-sociaux peuvent obtenir communication des éléments d'identification de leurs débiteurs en application de l'article L. 135 ZN du livre des procédures fiscales.

Le fournisseur de données procède à une série de contrôles, en amont de la restitution

des données, visant à limiter l'accès aux seules données autorisées pour le fournisseur de service concerné au regard des textes juridiques précisés dans sa demande de raccordement :

- la validité du certificat du fournisseur (un certificat SSL client authentifie l'administration et garantit la sécurisation du transfert des données) ;
- l'adresse IP de l'appelant ;
- la présence de l'identifiant technique de l'appelant ;
- l'identité du fournisseur de service ;
- le SPI ou NFP de l'usager.

Une fois ces contrôles effectués, les données conformes à la contractualisation entre le fournisseur de service et le fournisseur de données pourront être restituées.

Les données transmises sont stockées dans un silo sécurisé du fournisseur de service permettant de garantir leur confidentialité.

En revanche, si les vérifications opérées par le fournisseur de données ne sont pas conformes à la contractualisation, aucune donnée ne fera l'objet d'une transmission.

L'accès à l'API R2P s'effectue via l'API Management (APIM) qui constitue la plateforme de gestion des API de la DGFiP. L'APIM offre aux fournisseurs de services utilisateurs des API DGFiP des environnements de test et sécurise les appels effectués.

Un compte d'accès à la plateforme APIM sera généré et notifié au responsable technique mentionné dans le formulaire de souscription.

5. Les engagements des parties

5.1 Obligations du fournisseur de données

En tant que fournisseur de données, la DGFiP s'engage 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 R2P (publiée sur le « store » APIM de la DGFiP).

À ce titre, elle 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 fournisseur de service, données fiscales échangées…) est limitée et justifiée au regard du besoin pour lesquels elles sont collectées.

Par ailleurs, le fournisseur de données s'engage à fournir à ses partenaires fournisseurs de services 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 fournisseur de service

Il incombe au fournisseur de service de s'assurer de/du :

- respect de la réglementation relative à la protection des données à caractère personnel ;
- la validité et mise à jour des données de contact du responsable de traitement déclarées dans le « Data Pass » ;
- traitement des données échangées pour la ou les finalités déclarées par le biais du « Data Pass »;
- 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 fournisseur de données sous une forme littérale pour l'informer explicitement du dispositif d'échanges de données fiscales 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/personnels habilités des services compétents pour instruire les demandes des usagers. Le(s) service(s) destinataire(s) des données devront être expressément communiqués au fournisseur de données par le biais du « Data Pass »;
- 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 reposant sur la réalisation et la formalisation de contrôles périodiques, aléatoires ou ciblés ;
- **l'absence de stockage du SPI (ou NFP) au-delà du temps nécessaire au traitement de la demande de l'usager, sauf cadre juridique l'y autorisant.**

Il appartient au fournisseur de service 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. L'information doit intervenir dans un délai raisonnable avant la mise en œuvre de la délégation de service ou de la sous-traitance.

Le fournisseur de service doit également fournir par écrit au fournisseur de données toute information utile et nécessaire en cas d'événement de sécurité susceptible d'affecter la transmission des données ou les données elles-mêmes et ce, dans les meilleurs délais.

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 R2P, la DGFiP, fournisseur de données, ainsi que le fournisseur de service, opèrent 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.

La DGFiP est responsable des traitements :

1. de mise à disposition d'une API intermédiaire d'identification des personnes physiques à des fins de restitution du SPI ;
2. de mise à disposition d'une API d'identification des personnes physiques à des fins de fiabilisation des bases des états civils du partenaire.

Le fournisseur de service est responsable des traitements effectués dans le cadre de la collecte et l'utilisation des données transmises par la DGFiP.

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 modifiée (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 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 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, ces sous-traitants 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 échange de données, 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 présentant des risques 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 l'API R2P, chaque responsable de traitement s'engage à informer les autres responsables de traitement de ladite violation et à leur transmettre, le cas échéant, 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 Direction Générale des Finances Publiques traite les données à caractère personnel collectées :

- dans le formulaire de souscription en ligne « Data Pass » du site api.gouv.fr ainsi que
- dans le cadre de l'utilisation des API par les partenaires (logs et autres traces de connexion et d'utilisation, etc.) et les échanges subséquents avec le partenaire.

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 d'une autre source réglementaire spécifique.

Les données collectées dans le cadre de la souscription « Data Pass » sont conservées pendant 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 « Data Pass » : 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 vous estimez, après avoir contacté la DGFiP que vos droits ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

7. Coût du service

Aucune contrepartie financière n'est demandée par l'une ou l'autre des parties dans le cadre des échanges de données proposés par l'API R2P.

8. Sécurité

Dans le cadre des dispositions légales et réglementaires en matière de protection du secret et des données à caractère personnel, le fournisseur de service s'engage à prendre toutes les mesures utiles 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 OAuth 2.0 doivent être respectées dans l'implémentation des différentes briques du dispositif : https://tools.ietf.org/html/rfc6749 ;
- l'engagement du fournisseur de service 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 ;
- les parties doivent s'engager à couvrir les risques portant sur leur SI 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 ;
- 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.

Le partenaire conventionné est responsable des informations traitées dans le cadre du service, et à ce titre s'engage à respecter les obligations inhérentes à ce traitement, notamment celles relevant de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et 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 (RGPD).

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 : ex. isolation, 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 :
  - le cas échéant, activation d'une cellule de crise ;
  - restrictions temporaires d'accès ;
  - actions d'alerte (RSSI) réciproques et de communication.
- Résolution de l'incident :
  - analyse de l'incident de sécurité pour détermination de la cause, correction ;
  - vérification avant remise en service que l'élément malveillant a été supprimé et que les éventuelles vulnérabilités sont corrigées ;
- Le cas échéant : 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 du SI (comportements anormaux) incluant un système de traçabilité des accès et actions des utilisateurs y compris ceux automatisés par robot ou batch, sur les données et processus, ainsi qu' une politique de journalisation ;
- une revue des incidents faite régulièrement pour quantifier et surveiller les différents types d'incidents ;
- la mise en place d'une politique de journalisation et d'un bilan de traçabilité des actions des agents habilités à accéder aux données dans le cadre du présent dispositif ;
- la définition des acteurs, des circuits d'alerte, la sensibilisation des différents acteurs (utilisateurs, des exploitants …) ;
- 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 Data Pass

Pour toute question liée à la demande de souscription « Data Pass » à l'API R2P, une boîte aux lettres fonctionnelle est à disposition :

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

9.1.3 Contact du FS

Le FS précise les contacts à privilégier dans le cadre de sa demande de raccordement à l'API R2P formulée sur le formulaire « Data Pass ».

9.2 Volumétrie

Le quota d'appel par défaut est fixé à 50 appels par minute. Si le fournisseur de service souhaite disposer d'un quota d'appels supérieur à 50, il doit transmettre au fournisseur de données tout élément de volumétrie justifiant de ce besoin (pics de charge, nombre de dossiers à traiter et périodicité, …).

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 (MEP). 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 14 jours ouvrés avant leur application en conditions nominales et 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 d'architecture et des normes (SI1) 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 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 - Fournisseur de données, le profil DICP est le suivant :

D = 3-24h	I = 3	C = 3	P = 2

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.**

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 R2P : ouverture toute l'année ;
- Périodes sensibles identifiées : période de la télédéclaration (mi-avril à mi-juin) ;
- Plages d'ouverture du service : 24h/24h, 7/7j ;
- Offre de couverture de service de la DGFiP : 7h-20h ;
- Offre de couverture de service et le taux de disponibilité du téléservice est précisé par le partenaire conventionné lors de sa demande de raccordement à l'API R2P.

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 estimée 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

La DGFiP se réserve la liberté de faire évoluer, de modifier ou de suspendre, sans préavis, le service pour des raisons de maintenance ou pour tout autre motif jugé nécessaire. En pareille hypothèse, le fournisseur de service 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.

Le fournisseur de service peut bénéficier de l'échange de données tant que les données sont nécessaires au traitement de la demande de l'usager et que le texte juridique ou réglementaire qu'il fait valoir pour justifier l'accès à ces données est applicable.

Dans le cas contraire, celui-ci s'engage à en informer la DGFiP.

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

Les termes des présentes conditions d'utilisation 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 conditions générales d'utilisation fera l'objet d'une information auprès de la partie impactée.

Si une ou plusieurs des clauses des présentes conditions générales d'utilisation venai(en)t à être déclarée(s) nulle(s) 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 conditions générales 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 via l'API R2P, 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 R2P est maintenu conformément aux présentes conditions générales d'utilisation.

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 de service, les grèves, les pénuries, les émeutes, les incendies, les cas de force majeure, la guerre et le terrorisme.

Les présentes conditions générales d'utilisation 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 différend découlant des CGU, de leur interprétation ou application.

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