RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API R2P

(environnement de bac à sable)

Date de publication : 25 septembre 2020

FINANCES PUBLIQUES

Table des matières

1. Objet

Les présentes conditions générales d'utilisation (CGU) ont pour objet de définir les conditions d'utilisation de l'environnement de bac à sable 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 fiscales entre la DGFiP et un partenaire conventionné (administration, collectivité, établissement bancaire…).

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

Le raccordement à l'API R2P 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.

L'interface (ou API) R2P s'inscrit dans ce programme qui vise à encourager et à valoriser :

- la simplification des démarches administratives ;
- l'émergence de nouveaux services aux usagers ;
- l'échange de données détenues par les administrations.

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 (administration publique, collectivité locale, établissement bancaire...) qui sollicite le raccordement à l'API R2P dans le cadre des démarches en ligne qui sont proposées à l'usager 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

L'accès au dispositif API R2P est soumis à deux conditions cumulatives :

- la ou les information(s) recherchée(s) par le fournisseur de service doivent être strictement nécessaires au traitement d'une demande ou dans l'exercice des missions du fournisseur de service justifiant l'accès auxdites informations ;
- l'accès aux informations s'inscrit en application d'un texte législatif ou réglementaire.

Le fournisseur de service sollicitant le raccordement au dispositif doit être autorisé à demander et exploiter les données fiscales dans le cadre de l'exercice de ses missions.

À ce titre, un texte législatif ou réglementaire doit justifier l'accès à de telles données, être communiqué dans le cadre de la procédure de raccordement au fournisseur des données qui opère une analyse juridique systématique afin de déterminer si le partenaire conventionné est habilité à connaître ces données dans le cadre de ses missions.

Les textes justifiant l'accès aux données seront communiqués au fournisseur de données ainsi que la démarche concernée, le périmètre des données qui feront l'objet de l'échange, la durée et la volumétrie.

3.2 Déclaration d'accomplissement des formalités relatives à la protection des données à caractère personnel

Le fournisseur de service devra, en amont du raccordement, déclarer au fournisseur de données l'accomplissement des formalités en matière de protection des données à caractère personnel, en cochant la case à cet effet dans le formulaire de souscription en ligne « Data Pass ».

3.3 Homologation de sécurité

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

Le procès-verbal d'homologation sera demandé par le fournisseur de données avant

toute mise en production.

4. Description du dispositif de transmission des données

Le fournisseur de service peut interroger le fournisseur de données à partir de :

- état civil complet (nom, prénom, date et lieu de naissance) ;
- état civil dégradé et éléments d'adresse (les nom et prénom 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 (identifiant fiscal ou « numéro SPI).

L'accès à l'API s'effectue via l'API Management (APIM) qui constitue la plateforme de gestion des APIs de la DGFiP. L'APIM offre aux utilisateurs des APIs DGFiP des environnements de test pour toutes les API et sécurise les appels effectués. Un compte d'accès à cette plateforme 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 fictives 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).

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.

Par ailleurs, le fournisseur de données s'engage à fournir à ses partenaires toute information utile et nécessaire en cas d'événement de sécurité dans les meilleurs délais.

5.2 Obligations du fournisseur de service

Il incombera au fournisseur de service de s'assurer de l'absence de stockage du SPI au-delà du temps nécessaire au traitement de la demande de l'usager.

Il appartiendra 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 de son téléservice L'information devant intervenir avant la mise en œuvre de la délégation de service ou la sous-traitance.

Le fournisseur de service devra également fournir par écrit au fournisseur de données toute information utile et nécessaire en cas d'événement de sécurité dans les meilleurs délais.

6. 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.

7. Sécurité

Dans le cadre des dispositions légales et réglementaires en matière de protection du secret, 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'homologation du téléservice 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.

Dans le cadre du RGS, le partenaire conventionné veillera à procéder à l'homologation de sécurité du téléservice qui permet de demander les données fiscales (ordonnance n°2005-1516 du 8 décembre 2005, décret n°2010-112 du 2 février 2010).

L'homologation de sécurité de chacun des composants devra avoir été réalisée (DGFiP et partenaire conventionné) avant toute mise en production.

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) ;
- 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, des circuits d'alerte, la sensibilisation des différents acteurs (utilisateurs, des exploitants …) ;
- des tests des processus d'alerte.

8. Gestion des mises en production

8.1 Mise à disposition d'une boîte aux lettres fonctionnelle

8.1.1 Contact API R2P

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

bureau.capusagers-apimanagement@dgfip.finances.gouv.fr

8.1.2 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 ».

8.2 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 décrit dans le présent document. Suivi des mises en production du FD seul.

En matière d'information préalable sur les interventions programmées susceptibles de générer une indisponibilité ou une perturbation des applications, la DGFiP est dotée de l'outil GESIP (Gestionnaire des interventions programmées).

Plus précisément, l'outil vise à informer et à instruire les impacts des interventions sur la production. Son utilisation doit être systématique pour :

- l'ensemble des actions sur l'exploitation susceptible de générer une interruption de service ou d'avoir un impact sur la production (directement ou indirectement)
- toutes les interventions planifiées portant sur les infrastructures, qu'elles entraînent ou non une interruption de service
- l'ensemble des paliers majeurs prévus.

9. Les critères DICPA

La sous-direction Études et Développements (Bureau SI-1A) 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 et anonymat (DICPA).

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 DICPA. 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 R2P - Fournisseur de données, le profil DICPA est le suivant :

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

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.**
ANONYMAT	**A 1** Aucune donnée nominative identifiée.	**A 2** Traitement de données nominatives **internes à la DGFiP** : **- Pas d'exploitation** à des fins métier autres que celles prévues initialement ;	**A 3** Traitement de données nominatives **externes à la DGFiP** : **- Pas d'exploitation** à des fins métier autres que celles prévues initialement ;	**A 4** Besoin d'anonymat avéré : - **Interdiction** d'utiliser et d'exploiter des données directement ou indirectement nominatives ;

10. 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 : ouvert 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 %.

11. Suspension du service

Le fournisseur de données, en cas d'utilisation abusive du service, de manquement aux présentes conditions générales d'utilisation ou d'incident de sécurité, se réserve le droit de suspendre et/ou restreindre l'échange de données ayant lieu avec le fournisseur de service.

En pareil hypothèse, le fournisseur de service en sera dûment averti par écrit et dans les meilleurs délais.

12. Durée 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 le fournisseur de données selon les modalités décrites à l'article 13.

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

Toute modification des conditions générales d'utilisation fera l'objet d'une information auprès de la partie impactée avant que la modification ne soit effectuée.

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 avec 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.

14. Loi applicable et litiges

Les présentes conditions générales d'utilisation en langue française seront exécutées et interprétées conformément au droit français.

Tout litige qui ne pourra faire l'objet d'un règlement amiable sera soumis à la juridiction compétente.