RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API INFINOE

(environnement de bac à sable)

Date de publication : 23/05/2022

FINANCES PUBLIQUES

Historique des versions		
Date	**Version**	**Objet**
23/05/2022	v1.0	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
DataPass	Formulaire de souscription
DGFiP	Direction générale des Finances publiques
DTNum	Délégation à la transformation numérique
PA	Producteur d'API (au cas présent, la DGFiP)
CA	Consommateur d'API (au cas présent, le partenaire)
Production	Environnement de production (données réelles)
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

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 INFINOE de la Direction générale des Finances publiques (ci-après dénommée « DGFiP »).

L'API INFINOE est une interface permettant l'échange de données budgétaires, comptables et financières entre la DGFiP et un partenaire conventionné.

Elle récupère ainsi les données transmises par le 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 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 de souscription en ligne « 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 INFINOE permet à chaque organisme public national (partenaire conventionné) de transmettre les écritures budgétaires, comptables et financières à l'application INFINOE (Informations Financières des Organismes de l'État) développée par la Direction générale des Finances publiques.

Il s'agit d'une API d'écriture de données, exclusivement, où les données sont envoyées par les organismes publics nationaux à la DGFiP.

Dans ces conditions, l'API INFINOE permet d'enrichir les données de l'application INFINOE de données budgétaires, comptables et financières

La transmission de ces données par le biais de ce dispositif se fonde sur le décret

suivant : Décret n° 2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique.

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

2.2.1 Rôle du producteur d'API (PA)

Le producteur d'API est chargé de mettre à disposition du partenaire conventionné un service d'échange d'informations encadré par un texte législatif ou réglementaire. Dans le cadre de l'accès à l'API INFINOE, la DGFiP est le producteur d'API.

2.2.2 Rôle du consommateur d'API (CA)

Le consommateur d'API est le partenaire conventionné qui sollicite le raccordement à l'API afin d'échanger des informations avec le producteur d'API dans le cadre de ses obligations légales et réglementaires. Pour l'API INFINOE, l'organisme public national est le consommateur d'API.

3. Conditions d'accessibilité au dispositif

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

Par ailleurs, il est rappelé que l'interrogation de l'API, lorsqu'elle restituerait des éléments sensibles, serait couverte par la règle du secret professionnel prévue par les dispositions de l'article L. 103 du Livre des Procédures Fiscales, car elle contiendrait des données nominatives et personnelles. Il ne peut être dérogé au secret professionnel que par une disposition législative spécifique.

3.1 Conditions juridiques

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

- la ou les information(s) échangées avec le consommateur d'API doivent être strictement nécessaires au traitement d'une demande ou dans l'exercice des missions du consommateur d'API justifiant l'échange des dites informations;
- l'échange de données s'inscrit en application d'un texte législatif ou réglementaire.

Lorsque cela s'avère possible, le(s) texte(s) juridique(s) permettant de justifier la transmission des données doit être communiqué au producteur d'API dès la souscription à l'environnement bac à sable par le biais du formulaire « DataPass » en ligne.
En tout état de cause, cette communication devra intervenir au plus tard lors de la souscription à l'environnement de production par le biais du formulaire « DataPass » 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 producteur d'API.

De plus, des pièces justificatives supplémentaires devront être également transmises au producteur d'API selon la nature des relations entre les acteurs intervenant dans le cadre de la souscription au « DataPass » (demandeur, responsable de traitement et responsable technique).

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

Le consommateur d'API devra, en amont du raccordement, déclarer au producteur d'API l'accomplissement des formalités en matière de protection des données à caractère personnel, en cochant la case à cet effet dans le formulaire en ligne « DataPass » lors de la souscription à l'environnement de bac à sable.

Cette déclaration engage la responsabilité du consommateur d'API.

3.3 Homologation de sécurité

Le Référentiel général de sécurité (RGS) impose aux autorités administratives de réaliser des homologations de sécurité attestant formellement de la prise en compte de la sécurité de son système d'information.

Pour les consommateurs d'API ne relevant pas du champ d'application du RGS, un engagement sera néanmoins demandé quant à la mise en œuvre d'un processus offrant un niveau de garantie équivalent. Ainsi, dans la suite du document, le terme « homologation » désigne, pour ces entités, la démarche menée en ce sens.

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

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

Le consommateur d'API s'engagera à communiquer une nouvelle attestation d'homologation de sécurité à la fin de cette durée si celui-ci souhaite encore bénéficier du raccordement. À cette fin, le producteur d'API effectuera un rappel au consommateur d'API en lui indiquant la date d'expiration.

En l'absence d'une telle transmission, l'échange de données sera suspendu jusqu'à ce que le consommateur d'API communique ce document au producteur d'API. En l'absence persistante de transmission, cette suspension pourra être suivie d'une résiliation du contrat par le producteur d'API telle que visé à l'article 10 des présentes conditions générales d'utilisation.

4. Description du dispositif de transmission des données

L'accès à l'API INFINOE 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 consommateur d'API

Le consommateur d'API s'engage à échanger, les seules données fictives autorisées pour le cas d'usage concerné selon les modalités décrites dans la documentation fonctionnelle et technique de l'API INFINOE (publiée sur le « store » APIM).

Il appartient au consommateur d'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 de l'échange de données. L'information devant intervenir dans un délai raisonnable avant la mise en œuvre de la délégation de service ou la sous-traitance.

Le consommateur d'API doit également fournir par écrit au producteur d'API toute information utile et nécessaire en cas d'événement de sécurité susceptible notamment d'affecter le processus d'échange de données ou de porter atteinte à la disponibilité, la confidentialité ou l'intégrité des données et ce, dans les meilleurs délais.

5.2 Obligations du producteur d'API

Le producteur d'API est chargé d'instruire chaque demande de raccordement à l'API pour vérifier que ladite demande est éligible au dispositif.

Par ailleurs, le producteur d'API s'engage à fournir à ses partenaires conventionnés 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.

Au niveau de chaque API de la DGFiP, les éléments suivants des échanges sont tracés : l'horodatage, l'identifiant technique de l'usager transmis par le consommateur d'API, le verbe http, le code retour http, l'URI de la ressource de l'API et la complétude des paramètres de la requête.

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.

7. Sécurité

Dans le cadre des dispositions légales et réglementaires en matière de protection du secret et des données à caractère personnel, le consommateur d'API 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 de l'échange de données 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.

Lors de la souscription à l'environnement de bac à sable, le partenaire conventionné est responsable des informations échangées, 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).

Dans le cadre du RGS, le partenaire conventionné veillera à procéder à l'homologation de sécurité de l'échange de données entre la DGFiP et les établissements publics nationaux (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 tout accès à l'environnement de 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) 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 ;
- 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 APIM 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

8.1.2 Contact DTNum pour la souscription DataPass

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

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

8.1.3 Contact du consommateur d'API

Le consommateur d'API précise les contacts à privilégier dans le cadre de sa demande de raccordement à l'API formulée sur le formulaire « DataPass ».

8.2 Volumétrie

Par défaut, le quota d'appels de l'API est fixé à 50 appels par minute. Cette information sera fournie par le consommateur d'API lors de la souscription « DataPass » à l'environnement de production. S'il souhaite disposer d'un quota d'appels supérieur à 50, il devra transmettre au producteur d'API tout élément de volumétrie justifiant de ce besoin (pics de charge, nombre de dossiers à traiter et périodicité…).

8.3 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 décrit dans le présent document.

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 DICP

Le bureau de l'architecture et des normes (Bureau SI-1) 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 producteur d’API, 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.**

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 : ouverture toute l'année ;
- 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.

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 producteur d'API, 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 consommateur d'API.

En pareille hypothèse, le consommateur d'API 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 consommateur d'API peut bénéficier de ce dispositif d'échange tant que les données sont nécessaires au traitement de la demande et que le texte juridique ou réglementaire encadrant la transmission de données est applicable. Dans le cas contraire, celui-ci s'engage à en informer le producteur d'API.

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, 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 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.