RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API SATELIT

(environnement de production)

Date de publication : 17/ 10/2022

FINANCES PUBLIQUES

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
FD	Fournisseur de données (au cas présent, la DGFiP)
FS	Fournisseur de services (au cas présent, le partenaire)
PCR	Portail commun du recouvrement
Production	Environnement de production (données réelles)
Responsable de traitement	Personne physique ou morale, l'autorité publique, le service ou un 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

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 SATELIT de la Direction Générale des Finances Publiques (ci-après dénommé « DGFiP »).

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

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 nécessite de manière cumulative :

- la saisie, par le partenaire conventionné, dans le formulaire de souscription en ligne « DataPass », 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 » 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 « DataPass » validé ainsi que l'acceptation des conditions générales d'utilisation valent convention entre la DGFiP et le partenaire conventionné, au besoin précisé par des contrats et conventions spécifiques ad-hoc entre les partenaires.

2. Contexte et présentation du dispositif

2.1 Présentation du dispositif

L'API permet aux entités administratives (administration, ministère, organisme public, collectivité) et aux acteurs privés qui sont éligibles d'accéder aux données déclaratives, bancaires, de créances, de paiement, de remboursements, d'obligations fiscales ou d'habilitations d'un usager professionnel afin de permettre d'intégrer et de valider ces données dans leur système d'information.

Le détail des données échangées peut faire l'objet d'un contrat de service fonctionnel signé par les parties à l'échange de données, afin d'en préciser leur portée et leur interprétation.

Ce dispositif s'inscrit dans les travaux coordonnés par la Mission interministérielle « France Recouvrement » créée par le décret[1] n° 2019-949 du 10 septembre 2019, et en particulier pour les paragraphes 2 et 4 de son article 2.

Dans ces conditions, l'API restitue donc les données de la DGFiP conformément à l'objectif susvisé.

1 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039079555/

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, 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 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 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

Le fournisseur de service sollicitant le fournisseur de données doit être autorisé à demander et exploiter les données fiscales 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 un ou plusieurs textes juridiques qui doivent justifier ledit accès.

En effet, ce(s) texte(s) doit/vent permettre au fournisseur de données, de vérifier l'existence d'un fondement légal justifiant la demande et la communication des données au fournisseur de service ainsi que le périmètre des informations sollicitées par ce dernier.

En fonction de la qualité du fournisseur de service et de l'usage pour lequel sont sollicitées les données, le(s) fondement(s) juridique(s) diffère(nt).

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

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

La communication du(des) texte(s) juridique(s) permettant de justifier l'accès aux données 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 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 « DataPass » (demandeur, responsable de traitement et responsable technique).

La conformité à ces exigences de complétude juridique peut être effectuée par tout moyen, y compris par contractualisation ad-hoc de niveau supérieur entre le fournisseur de données et le fournisseur de service.

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

Le fournisseur de service doit, 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 en ligne « DataPass » lors de la souscription à l'environnement de production.

Cette déclaration engage la responsabilité du fournisseur de service.

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 fournisseurs de service ne relevant pas du champ d'application du RGS, un engagement est 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 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.

L'homologation de sécurité vaut pour une durée maximale de cinq (5) ans.

Le fournisseur de service s'engage 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 fournisseur de données effectuera un rappel au fournisseur de services 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 fournisseur de service communique ce document au fournisseur de données. En

l'absence persistante de transmission, cette suspension peut être suivie d'une résiliation du contrat par le fournisseur de données telle que visé à l'article 14 des présentes conditions générales d'utilisation.

4. Description du dispositif de transmission des données

En fonction du cadre juridique, et fonction des contrats d'interfaces publiés, le fournisseur de service peut interroger le fournisseur de données à partir de :

- SIREN
- IDOCFI après son obtention sur la base du SIREN
- IdPCR (identifiant technique de l'usager du FS quand ce dernier intègre la fédération d'identité PCR)

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 ;
- les droits du fournisseur de service sur les données demandées pour l'année concernée.

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, si un besoin de stockage, même temporaire, est justifié par le fournisseur de service. Les durées de stockage des données transmises ne devront pas excéder celles prescrites par le fournisseur de données. Ces prescriptions incluent les directives de mises en caches renvoyées par les API.

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 s'effectue via l'API Management (APIM) qui constitue la plateforme de gestion des API de la DGFiP. L'APIM offre aux utilisateurs des API 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 « DataPass ».

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 (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.

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 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 fournisseur de service, le verbe http, le code retour http, l'URI de la ressource de l'API et la complétude des paramètres de la requête.

5.2 Obligations du fournisseur de service

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

- la communication et du respect de la déclaration d'accomplissement des formalités liées à 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 « 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 fournisseur de données sous une forme littérale pour l'informer explicitement du dispositif d'échanges de données fiscales pour la démarche envisagée ;
- 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 ;
- 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 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 dans un délai raisonnable 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 susceptible notamment 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, 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.

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).

Dans l'hypothèse où les fournisseurs de données et de service seraient qualifiés de responsables conjoints de traitement, au sens de la réglementation relative à la protection des données à caractère personnel, dans le cadre de l'échange de données par le biais de l'API, il conviendra de se reporter à la convention de coresponsabilité qui aura été établie et qui définit spécifiquement leurs obligations respectives.

6.2 Confidentialité

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

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.

Si les sous-traitants ne remplissent pas leurs obligations en matière de protection des données, les responsables de traitement, demeurent chacun pour ce qui les concerne pleinement responsables de l'exécution de ces obligations par ces derniers.

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 après en avoir pris connaissance 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, 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.

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.

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'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 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 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 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.

La définition opérationnelle de ce processus de sécurité fait l'objet d'une annexe au conventionnement de production, convention mentionnée infra aux points 10 et 11.

9. Gestion des mises en production

9.1 Identification des points de contact

9.1.1 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

9.1.2 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

9.1.3 Contact du FS

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

Ces points de contacts sont, le cas échéant, précisés dans le détail dans le Contrat de service fonctionnel entre projets et dans le conventionnement de production pour les acteurs associés.

9.2 Volumétrie

Par défaut, le quota d'appels de l'API en environnement de production est fixé à 500 appels par minute. Cette information est fournie par le fournisseur de service lors de la souscription « DataPass » à l'environnement de production. S'il souhaite disposer d'un quota d'appels supérieur à 500 appels par minute, 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

Le suivi des mises en production fait l'objet d'un conventionnement spécifique entre les parties. Dans le cas où il ne serait pas conclu à la souscription, le niveau de service décrit ci-après s'applique par défaut.

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.

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.

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 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 précisé dans la convention de service spécifique de production entre les parties. A défaut de signature à la date de souscription, le DICP suivant est assuré.

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 qualité de service fait l'objet d'un conventionnement spécifique de production entre les parties. Dans le cas où il ne serait pas conclu à la souscription, le niveau de service ci-après s'applique par défaut.

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 : 0h-24h, 7/7j (service non disponible pour maintenance sur une plage de 2h entre 23h et 6h) ;
- 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 %.

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

13. 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 suivant.

14. 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.

15. 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.