RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API Impôt particulier

avec connexion FranceConnect

(environnement de production)

Date de publication : 25 septembre 2020

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 production de l'API Impôt particulier de la Direction Générale des Finances Publiques (ci-après dénommée « DGFiP ») dans le cadre du téléservice FranceConnect.

L'API Impôt particulier est une interface permettant l'échange de données fiscales entre la DGFiP et un partenaire conventionné (administration, collectivité...).

Elle met ainsi à disposition certaines données fiscales strictement utiles à une ou plusieurs démarches proposées aux usagers.

Le raccordement à l'API Impôt particulier 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 d'échange de données

2.1 Présentation du dispositif

Le programme « Dites-Le Nous Une Fois » vise à simplifier les démarches administratives et à améliorer les relations entre les usagers et l'administration, en les dispensant d'avoir à fournir plusieurs fois la même information à différentes administrations.

Il s'inscrit dans le cadre de la mise en œuvre des articles L. 114-8 et suivants du Code des Relations entre le Public et l'Administration (CRPA) relatifs aux échanges de données entre administrations, créés par l'ordonnance n°2015-1341 du 23 octobre 2015, modifié par la loi n°2016-1321 du 7 octobre 2016 – art. 91.

Aussi, l'interface (ou API) Impôt particulier 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.

L'échange de données via l'API Impôt particulier s'effectue sur la base des textes juridiques suivants :

- les articles L.114-8, L-100-3 du Code des Relations entre le Public et l'Administration (ci-après dénommé « CRPA ») ;
- le décret n° 2019-33 du 18 janvier 2019, fixant la liste des pièces justificatives que

le public n'est plus tenu de produire à l'appui des procédures administratives ;

- le texte législatif autorisant le fournisseur de service à demander et à exploiter l'accès aux données fiscales de l'usager par le biais de l'API Impôt Particulier

Le dispositif s'appuie sur le service FranceConnect qui est un mécanisme de fourniture d'identité et d'authentification numérique pour les usagers, à savoir que le transfert de données fiscales par API ne s'effectue que lorsque l'usager s'est préalablement authentifié avec FranceConnect et a consenti à l'échange.

Le dispositif fait ainsi intervenir l'opérateur de FranceConnect, un fournisseur d'identité, un fournisseur de service et un fournisseur de données .

2.2 Les acteurs intervenant dans le dispositif d'échange de données

2.2.1 Le rôle du fournisseur d'identité (FI)

Le fournisseur d'identité est chargé de transmettre à FranceConnect l'identité de l'usager qui s'est authentifié chez lui avec les identifiants du compte qu'il possède chez ce fournisseur. La DGFiP est fournisseur d'identité ; d'autres fournisseurs d'identité sont associés au projet FranceConnect comme La Poste ou AMELI.

Dans le cadre de l'accès à l'API Impôt particulier, la direction interministérielle du numérique (ci-après « DINUM ») agit en tant qu'opérateur de FranceConnect.

2.2.3 Le 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 couvert du consentement préalable et explicite de l'utilisateur.

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

2.2.2 Le rôle du fournisseur de service (FS)

Le partenaire conventionné (administration publique, collectivité locale, établissement bancaire...) qui sollicite le raccordement à l'API Impôt particulier 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 Impôt Particulier se réalise sur le site www.api.gouv.fr par le biais du formulaire « Data Pass » dans le cadre du téléservice FranceConnect. 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 raccordement au dispositif doit être autorisé à demander et exploiter les données fiscales dans le cadre de l'instruction de démarches administratives.

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.

Conformément au Code des relations entre le public et l'administration (CRPA), l'échange de données s'impose en effet aux administrations dès lors que :

- ces données sont nécessaires au traitement d'une demande présentée par un usager ;
- et que l'administration destinataire est habilitée à connaître ces données dans le cadre de ses missions.

Les textes justifiant l'accès aux données devront être 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

Pa ailleurs, 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 de souscription en ligne « Data Pass ».

3.3 Information de l'usager

Dans le cadre de l'échange de données opéré, l'usager dispose d'un droit d'information en vertu de l'article L.114-8 du CRPA et de la réglementation relative à la protection des données à caractère personnel. Il incombe ainsi au fournisseur de service de porter à la connaissance de l'usager l'ensemble des mentions prescrites par les textes précités en des termes clairs et aisément compréhensibles et notamment le fait que le fournisseur de service se procure directement les données auprès du fournisseur de données, c'est-à-dire la DGFiP.

3.4 Consentement de l'usager préalable à l'échange de données

L'administration ou l'organisme qui accède aux données de l'API Impôt particulier doit au préalable avoir recueilli le consentement de l'usager. Le consentement recueilli doit ainsi être libre, spécifique, éclairé et univoque pour être valable.

3.5 Homologation de sécurité

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

Le procès-verbal d'homologation est demandé par le fournisseur de données avant toute mise en production.

4. Déroulement du processus de transmission des données par le fournisseur de données au fournisseur de service

Lorsque l'usager effectue sa démarche administrative sur le site du fournisseur de service, il doit s'authentifier via le bouton FranceConnect présent sur la page du fournisseur de service en choisissant un fournisseur d'identité comme la DGFiP. L'usager remplit le formulaire de demande de démarches en ligne sur le site du fournisseur de service qui lui propose d'aller récupérer directement les informations fiscales nécessaires au traitement de son dossier.

Il autorise ce dernier à récupérer les seules données fiscales nécessaires pour le traitement de ladite démarche en donnant son consentement après avoir été informé de la nature et de l'origine des données concernées.

FranceConnect transmet au fournisseur de données le jeton technique qui permet de récupérer les éléments (l'état civil, le(s) « scope (s)») utiles pour l'identification de l'usager et l'échange de données.

Le fournisseur de données contrôle les éléments suivants pour s'assurer que la demande du fournisseur de service est fondée :

- le certificat de chaque fournisseur de service par l'intermédiaire de l'URL d'appel utilisée par le FS ;
- la validité du consentement auprès de FranceConnect au moyen du jeton fourni par FranceConnect ;
- l'identité de l'usager ;
- le SPI retourné ;
- le fait que le fournisseur de service dispose effectivement des droits 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 la DGFiP pourront être restituées au FS.

En cas de rejet de la demande, le traitement s'arrête et aucune donnée n'est transmise. Aucune donnée fiscale n'est envoyée à FranceConnect.

Dans le cadre de l'échange par FranceConnect, les données transmises par la DGFiP sont affichées sur la page de consentement sous la forme littérale suivante (avec l'ajout de l'origine de la donnée).

Les données transmises par le fournisseur de données sont stockées dans un silo sécurisé du fournisseur de service.

5. Les engagements de chacune des parties

5.1 Engagements de la DINUM

Dans le cadre de l'API Impôt Particulier, il incombe à la DINUM la mise en œuvre et le pilotage du service « FranceConnect ».

Elle doit prendre en charge le consentement explicite de l'usager concernant la transmission et le traitement de ses données fiscales dans les conditions exposées ci-

dessus.

Si l'un des partenaires de FranceConnect, aussi bien fournisseur de service que fournisseur d'identité est compromis, la DINUM s'engage alors à couper les liens entre FranceConnect et le fournisseur concerné, tout en informant les partenaires dans les meilleurs délais. Le système ne sera rétabli qu'une fois la sécurité du partenaire garantie et validée par le RSSI de la DINUM.

La disponibilité du téléservice offert est dite « forte » selon les critères de la DGFiP. Les exigences relatives à ce niveau de disponibilité sont explicitées dans le présent document.

La DINUM s'engage à fournir à ses partenaires toute information utile et nécessaire en cas d'événement de sécurité, dont notamment l'ensemble des journaux techniques qui permettraient la corrélation des événements de sécurité avec le SI du fournisseur de données.

La DINUM s'engage à informer par écrit les partenaires préalablement à toute modification des paramètres de sécurité.

La DINUM conserve les données de traçabilité pour une durée de trente-six (36) mois à compter de la dernière session.

5.2 Engagements du fournisseur de données

La DGFiP en sa qualité de fournisseur de données, s'engage à transmettre, pour l'usager concerné, les données autorisées pour le cas d'usage du téléservice et ce en respectant l'implémentation rigoureuse des règles d'appels.

A ce titre, elle est en charge d'une part, d'instruire chaque demande de raccordement à l'API pour vérifier que ladite demande est éligible au dispositif et d'autre part d'assurer un certain nombre de contrôles qui sont exposées au sein de la description du déroulement du processus de transmission des données

Le fournisseur de données conserve les données de l'échange (identification de l'usager qui fait l'objet de la demande, identification du partenaire, données fiscales échangées…) deux (2) ans à compter de la date de réception de la demande.

Il appartient au e fournisseur de données de communiquer à ses partenaires toute information utile et nécessaire en cas d'événement de sécurité dans les meilleurs délais.

5.3 Engagements du fournisseur de service

Dans le cadre du raccordement à l'API Impôt Particulier, le fournisseur de service s'engage à mettre en œuvre le service conformément aux dispositions légales et réglementaires ainsi qu'aux documents mentionnés plus haut. En particulier, tous les éléments d'information nécessaires pour l'utilisation du service FranceConnect seront présentés à l'usager.

Il incombe au fournisseur de service d'assurer :

- la communication et le respect de la déclaration d'accomplissement des formalités liées à la réglementation relative à la protection des données à caractère personnel ;
- l'affichage de l'information devant être portée à la connaissance de l'usager afin que celui-ci puisse donner son consentement en toute connaissance de cause,

dans les conditions et modalités prescrites par l'article 2 des présentes conditions générales d'utilisation ;

- l'affichage explicite du consentement valide intégré nativement dans FranceConnect permettant le transfert des données, intégrant la nature et l'origine des données fiscales ;
- l'accès aux données échangées aux seuls agents/personnels habilités des services compétents pour instruire les demandes des usagers ;
- la mise en œuvre de toutes les mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité, l'intégrité et la confidentialité des données ;
- l'accompagnement de l'usager, par la possibilité dans chaque écran d'accéder aux mentions légales précisant les droits dont dispose l'usager ainsi que les modalités d'exercice de ces derniers et de mise en relation avec un interlocuteur.

Le fournisseur de service devra 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.

Celui-ci s'engage à fournir à ses partenaires toute information écrite, utile et nécessaire en cas d'événement de sécurité et ce, dans les meilleurs délais.

6. Protection des données à caractère personnel échangées

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 Impôt particuliers, la DGFiP, fournisseur de données, la DINUM, fournisseur de connexion ainsi que le fournisseur de service, opèrent des traitements de données à caractère personnel.

A ce titre, chacun agit en sa qualité de responsable de traitement pour des 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 dénommée la « réglementation »).

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 Relation 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 Devoir de 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

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 risques pour les droits et libertés des personnes concernées en rapport avec l'exécution du téléservice dans les soixante-douze 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 faisant l'objet des présentes conditions générales d'utilisation, 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 sa part de responsabilité dans celui-ci.

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 Impôt particulier.

8. Sécurité

Dans le cadre des dispositions légales et réglementaires en matière de protection du secret, les partenaires s'engagent 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.

L'implémentation rigoureuse des règles d'appels telles que définies dans l'annexe « Processus d'implémentation de FC par FS » des conditions générales d'utilisation de FranceConnect en conformité avec le Référentiel Général de Sécurité (RGS) est obligatoire pour tout échange.

Dans le cadre du RGS, le FS 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 (DINUM, DGFiP et FS) 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.

9. Protocole d'échanges en production entre FranceConnect et la DGFiP

Ce protocole spécifie les modalités opérationnelles de la collaboration entre les services en production pour établir des échanges de données entre les fournisseurs de service (FS) proposés par FranceConnect, opéré par la DINUM, et le fournisseur de données mis à disposition par la DGFiP.

9.1 Gestion des mises en production

9.1.1 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'urgences.

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

9.1.2 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.

Le dispositif de la DGFiP intègre la brique FC au sein de l'outil GESIP. Cette intégration dans l'outil de suivi de la DGFiP permet une diffusion par courriel aux points de contacts définis par la DINUM (cf. adresse mail fonctionnelle mentionnée ci-après).

Le processus de communication de GESIP permet d'informer les interlocuteurs désignés à la DINUM des mises en production de la DGFiP pouvant affecter FC comme, par exemple :

- API ADONIS
- API Management
- Authentification SSO DAC
- PAS BIANCA
- PERS ZU
- SINF ZU

9.1.3 Suivi des mises en production du FC seul

Lors de toute évolution FC, en l'absence d'outil dédié de la DINUM le partage de l'information implique nécessairement une communication écrite par courriel. L'utilisation du téléphone entre les parties est à réserver aux mises en production urgentes. Les changements doivent être annoncés 14 jours ouvrés avant leur application en conditions nominales et 7 jours ouvrés avant leur application en cas d'urgences.

9.1.4 Suivi des mises en production du FC et FD

Dans le cas des mises en production coordonnées concernant les deux briques (FC et FD), la complexité technique ainsi que le nombre plus élevé d'opérateurs en interactions plaident pour la mise en place d'un pilotage commun et concerté, par exemple dans le cadre d'une feuille de route.

Toujours dans ce contexte, un GO commun à la mise en production sera prononcé dans le cadre d'une instance rassemblant les deux parties.

La communication de la DGFiP autour de la MEP sera assurée par les outils GESIP et SWITCH (cf.supra) renforcée par courriel si nécessaire.

La DINUM assurera la communication autour de la MEP par courriel sur la base des contacts de la liste fournie dans le document .

Des échanges autour d'un calendrier prévisionnel des MEP sont à mettre en place. Chaque partie mettra en place une information mensuelle des MEP connues pouvant potentiellement impacter le FI ou le FD dans les deux mois à venir.

9.2 Gestion des incidents

9.2.1 Modalités de traçabilité et de communication sur les incidents

Il n’y a pas d’outil partagé avec les partenaires sur la traçabilité et le suivi des incidents. Ce partage est assuré par une communication par courriel entre les parties.

Les contacts nécessaires à cette communication figurent au présent document.

Les deux parties s’engagent à ne pas communiquer ces points de contact aux usagers.

En cas de dysfonctionnement, les parties mettront en œuvre tous les moyens dont ils disposent pour rétablir une situation normale dans les meilleurs délais.

La garantie du temps de rétablissement en cas d'incident est estimée à 24 heures ouvrées (Critères DICPA décrits dans le présent document).

Tous les incidents causant une rupture ou risquant de rompre les services en ligne considérés sont tracés. Pour chaque incident faisant l'objet d'une remontée, il conviendra de préciser :

- L’impact de l’incident sur le service aux utilisateurs,
- L’urgence qui reflète l’évaluation de la rapidité avec laquelle un incident doit être résolu, en solution définitive ou de contournement.

9.2.2 Suivi des incidents du FD seul

Une procédure a été mise en place à la DGFiP, dans le cadre de la gestion d’événements

ou d'incidents d'exploitation se traduisant pour les utilisateurs par des indisponibilités ou des dégradations de services.

Le dispositif intègre l'utilisation de l'outil SWITCH (Service Web d'Information et de Transmission pour une Communication Harmonisée) dans le processus de communication vers la DINUM Ce dernier, permet la mise en place de :

- la communication sur les dysfonctionnements, perturbations ou incidents d'exploitation d'une application ayant un impact sur les utilisateurs
- l'information sur la mise en oeuvre effective des interventions programmées susceptibles de générer une indisponibilité ou une perturbation des applications.

Le processus sera activé par la DGFiP lorsque la rupture de service du FD dépassera le délai de 20 minutes.

9.2.3 Suivi des incidents du FC seul

Du fait de l'absence d'outil dédié de la DINUM le partage de l'information implique nécessairement une communication écrite par courriel auprès des contacts recensés.

En cas d'indisponibilité non planifiée de la brique FranceConnect supérieure à 20 minutes une alerte sera transmise à la DGFiP afin de lui signaler l'incident en cours.

9.2.4 Gestion avancée d'incident / gestion de crise FC et FD

Dans le cas d'un incident concernant les deux briques (FC et FD), la complexité technique ainsi que le nombre plus élevé d'opérateurs impactés plaident pour la mise en place d'une concertation des pilotages. Après un contact bilatéral entre les pilotages de production, un point audio pourra être ouvert afin de piloter les actions de résolution.

La communication de la DGFiP sera assurée par SWITCH (cf.supra) et renforcée par courriel.

La DINUM assurera la communication autour de l'incident par courriel. Les échanges se feront sur la base des contacts de la liste fournie.

9.3 Contacts dans la gestion des incidents

9.3.1 Contact FranceConnect

Pour toute question liée à FranceConnect, la DINUM met à disposition de 9h00 à 18h00 sauf week-ends et jours fériés, l'adresse électronique support@dev-franceconnect.fr

Les messages SWITCH seront adressés à la DINUM à l'adresse support@dev-franceconnect.fr

9.3.2 Contact API Impôt particulier

Pour toute question liée à l'API Impôt particulier, une boîte aux lettres fonctionnelle est à disposition impot.particulier@api.gouv.fr

9.3.3 Contact Pôle données

Pour toute question liée à la demande de souscription à l'API Impôt particulier, une boîte aux lettres fonctionnelle est à disposition bureau.capusagers-pole.donnees-dgfip@dgfip.finances.gouv.fr

9.3.4 Contact API Management

Pour toute question liée à l'API Management, une boîte aux lettres fonctionnelle est mise à disposition bureau.capusagers-apimanagement@dgfip.finances.gouv.fr

9.3.5 Contact du FS

Le FS précise les contacts à privilégier dans le cadre de sa demande de raccordement à une API.

10. 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 FranceConnect – 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 ;

11. La qualité de service

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

- FranceConnect et API Impôt particulier : ouvert toute l'année ;
- Périodes sensibles identifiées : période de la télédéclaration (mi-avril à mi-juin) ;
- Plages d'ouverture du service pour les usagers : 24h/24h, 7/7j ;
- Offre de couverture de service du FD DGFiP : 7h-20h ;
- Offre de couverture de service de FranceConnect : 7h-20h ;
- Taux de disponibilité : 99,9 % pour la DINUM ;
- Offre de couverture de service et le taux de disponibilité du téléservice est précisé par le FS lors de sa demande de raccordement à l'API Impôt particulier.

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 pareil 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 14.

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

Toute modification des présentes conditions générales d'utilisation fera l'objet d'une information auprès des parties impactées avant que la modification ne soit effectuée.

Par ailleurs, si l'une des parties souhaite mettre fin à l'échange de données avec l'API Impôt particulier, elle en informe les partenaires 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 Impôt particulier 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.

16. Autres documents contractuels

Dans la mesure où l'échange de données fiscales via l'API Impôt particulier, objet des présentes conditions générales d'utilisation, ne s'effectue que lorsque l'usager s'est préalablement authentifié avec FranceConnect, les prérequis pour l'ensemble des acteurs sont :

- Le FI devra respecter les contraintes techniques liées à FC précisées dans le document accessible à l'adresse suivante : https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-identite
- Le FS devra respecter les contraintes techniques liées à FC précisées dans le document accessible à l'adresse suivante : https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-service
- Le FD devra respecter les contraintes techniques liées à FC précisées dans le document accessible à l'adresse suivante adresse : https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-donnees
- Les conditions générales d'utilisation du service FranceConnect entre le DINUM et le FS ou le FI sont accessibles à l'adresse suivante : https://partenaires.franceconnect.gouv.fr/cgu