VERSION DE TRAVAIL

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Convention de partenariat entre la Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État (DINSIC), la Direction Générale des Finances Publiques (DGFiP) et la $NomDuFS

en vue de la mise à disposition de l'API « Impôt Particulier »

Entre :

La Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État (DINSIC), représenté par M. Henri Verdier, 64 allée de Bercy, 75 012 Paris, en charge de FranceConnect

Et :

La Direction Générale des Finances Publiques (DGFiP), au Ministère de l'Action et des Comptes publics, représentée par $RepresentantDGFiP 139, Rue de Bercy 75 012 Paris, et désigné, ci-dessous « Fournisseur de données »,

Et :

$NomDuFS, représenté(e) par $RepresentantDuFS et désigné ci-dessous « Fournisseur de services »,

Il est convenu ce qui suit :

-Vu l'arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect »

– Vu la délibération n° 2015-254 du 16 juillet 2015 portant avis sur un projet d'arrêté portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect » (demande d'avis n° 15012943)

– Vu l'arrêté du 1er septembre 2016 portant création par la Direction générale des finances publiques d'un traitement automatisé de données à caractère personnel dénommé « module applicatif d'interrogation de données »

– Vu la délibération n°2016-261 du 21 juillet 2016 portant avis sur un projet d'arrêté portant modification d'un traitement automatisé d'informations nominatives dénommé « accès au dossier fiscal des particuliers (ADONIS) » (demande d'avis n° 1975621)

– Vu le $NatureDuFondementLegal $ReferenceDuFondementLegal autorisant le fournisseur de service à demander les données fiscales à la DGFiP pour le téléservice « $NomDuTeleservice »

I – Préambule

1.1 Les enjeux

Le programme « Dites-le nous une fois – Particuliers », 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 L114-8 et suivants du Code des Relations entre le Public et l'Administration relatifs aux échanges de données entre administrations, créés par l'ordonnance n°2015-1341 du 23 octobre 2015.

L'API « Impôt Particulier » relève de ce programme et vise à encourager et à valoriser :

- la simplification des démarches administratives ;
- le prototypage et l'émergence de nouveaux services aux usagers ;
- l'exposition des données détenues par les administrations ;

et à soutenir la fabrication de nouveaux services innovants et répondant aux besoins des usagers ainsi qu'aux décisions de simplification.

1.2 Description du dispositif de transmission des données via l'API « impôt particulier »

L'API « Impôt Particulier » a été développée pour permettre aux usagers d'effectuer une démarche administrative en ligne sans avoir à fournir de justificatifs fiscaux sous forme papier.

L'échange de données fiscales s'appuie sur le service FranceConnect qui est un mécanisme de fourniture d'identité et d'authentification numérique pour les usagers. C'est ainsi que le transfert de données fiscales par API ne s'effectue que lorsque l'usager s'est préalablement authentifié avec FranceConnect.

Le dispositif fait intervenir les acteurs suivants : l'opérateur FranceConnect (FC), un fournisseur d'identité (FI), un fournisseur de services (FS) et un fournisseur de données (FD).

1.3 Le rôle des différents acteurs de l'environnement FranceConnect

1.3.1. Le rôle du fournisseur d'identité

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.

1.3.2. Le rôle du fournisseur de services

Le fournisseur de services est un site internet qui propose à l'usager d'effectuer des démarches en ligne.

1.3.3 Le rôle du fournisseur de données

Le fournisseur de données est chargé de transmettre un ensemble d'informations à un fournisseur de services dûment habilité sous couvert du consentement préalable et explicite de l'utilisateur.

II – Documents contractuels

Dans la mesure où l'échange de données fiscales via l'API « Impôt Particulier », objet de la présente convention, 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://franceconnect.gouv.fr/fournisseur-identite

– Le FS devra respecter les contraintes techniques liées à FC précisées dans le document accessible à l'adresse suivante : https://franceconnect.gouv.fr/fournisseur-service

– Le FD devra respecter les contraintes techniques liées à FC précisées dans le document accessible à l'adresse suivante : https://franceconnect.gouv.fr/fournisseur-donnees

– Les conditions générales d'utilisation du service FranceConnect entre la DINSIC et le FS ou le FI sont accessibles à l'adresse suivante : https://franceconnect.gouv.fr/cgu (version $VersionDesCGUFC du $DatedeVersiondesCGUFC).

La présente convention est également constituée des annexes suivantes, lesquelles ont une valeur juridique identique :

ANNEXE 1 : Description des données transmises par la DGFiP

ANNEXE 2 : Qualité de service

ANNEXE 3 : Modalités d'utilisation de l'API « Impôt Particulier » – Contrat de service technique

ANNEXE 4 : Protocole d'échanges en production entre FranceConnect et la DGFiP fournisseur de données.

ANNEXE 5 : Sécurité

Mise à jour des annexes :

Les Parties à la présente convention s'engagent à se signaler mutuellement, dans les meilleurs délais, toute modification totale ou partielle des annexes pré-citées.

Article 1. Objet de la convention

Le présent document a pour objet de définir les conditions de collaboration entre la DINSIC, le fournisseur de services et la DGFiP dans le cadre de la mise à disposition de l'API « Impôt Particulier » via FranceConnect pour le téléservice « $NomDuTeleservice ».

Article 2. L'échange de données

Dans le cadre de l'accès à l'API « Impôt Particulier » pour le cas d'usage visé à l'article 1, la DINSIC agit en tant qu'opérateur de FranceConnect, le $NomDuFS en tant que fournisseur de services (FS) et la DGFiP en tant que fournisseur de données (FD) et potentiellement en tant que fournisseur d'identité (FI).

Les informations fiscales échangées entre la DGFiP et le fournisseur de services figurent dans les offres de service décrites dans l'annexe 1.

Article 3. Durée de la convention

La présente convention est exécutoire dès la signature par les parties.

Elle est conclue pour une durée de 5 ans, renouvelable par tacite reconduction.

Les parties pourront dénoncer cette convention dans les conditions et selon les modalités définies à l'article 10.

La DGFiP peut toutefois y mettre fin à tout moment si les conditions ayant permis la mise en œuvre de l'échange ne sont plus réunies.

Article 4. Rôle et engagements de la DINSIC

La DINSIC met en œuvre et pilote le service « FranceConnect ».

La DINSIC prend en charge le consentement explicite de l'usager quant à la transmission et au traitement de ses données.

Si l'un des partenaires de FranceConnect, aussi bien fournisseur de services que fournisseur d'identité est compromis, la DINSIC 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 DINSIC.

La disponibilité du téléservice offert est dite « forte » selon les critères de la DGFiP. Les exigences relatives à ce niveau de disponibilité sont explicitées en annexe 2.

La DINSIC est responsable des informations traitées dans le cadre de FranceConnect 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.

La DINSIC et le fournisseur de service s'engagent à fournir à leurs 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 DINSIC s'engage à informer les partenaires préalablement à toute modification des

paramètres de sécurité.

La DINSIC conserve les données de traçabilité pour une durée de trente-six mois à compter de la dernière session.

Article 5. Rôle et engagements de la DGFiP

En tant que fournisseur de données, la DGFiP s'engage à transmettre, pour l'usager concerné, les données indiquées à l'annexe 1 en respectant l'implémentation rigoureuse des règles d'appels telles que définies dans la documentation en ligne précédemment citée.

La durée de conservation des traces de l'échange (identification de l'usager qui fait l'objet de la demande, identification du partenaire, données fiscales échangées…) est de 2 ans, conformément à ce qui est décrit dans les dossiers CNIL déposés par la DGFiP (FranceConnect et API « Impôt Particulier »).

La DGFiP s'engage à fournir à ses partenaires toute information utile et nécessaire en cas d'événement de sécurité.

Article 6. Rôle et engagements du fournisseur de services (FS)

Le fournisseur de services met en œuvre et opère le service conformément aux dispositions légales et réglementaires au sens de l'article 4 de l'arrêté du 24 juillet 2015, ainsi qu'aux documents mentionnés supra. En particulier tous les éléments d'information nécessaires pour l'utilisation du service FranceConnect seront présentés à l'usager.

Conformément au règlement général sur la protection des données (RGPD) en vigueur depuis le 25 mai 2018, le fournisseur de services s'engage à se conformer aux principes fondamentaux de la protection des données à réaliser l'étude d'impact associée avant la mise en production de son téléservice.

La mise en œuvre de la fonctionnalité FranceConnect a fait l'objet d'un arrêté du 24 juillet 2015 et d'une délibération de la CNIL n° 2015-254 du 16 juillet 2015 (demande d'avis n° 15012943).

Dans le cadre du téléservice, le fournisseur de service susmentionné s'engage à s'assurer :

– que la liste et l'origine des données transmises soient affichées sur la page de consentement de l'usager ;

– de la bonne utilisation des données personnelles ;

– du respect de la confidentialité des données ;

– de la mise en œuvre de tous les moyens nécessaires à leur garantie ;

– de l'accompagnement de l'usager, par la possibilité dans chaque écran d'accéder aux mentions légales précisant les possibilités de rectification des données, de permettre la mise en relation de l'usager avec un interlocuteur (adresse courriel), et d'indiquer une rubrique contact accessible dans tous les menus.

Il est responsable du respect et de la bonne mise en œuvre de la réglementation édictée par l'Agence Nationale de la sécurité des systèmes d'information (ANSSI) que ce soit sur les domaines de la protection des systèmes d'informations, de la confiance numérique (RGS, eIDAS), de la réglementation technique et cryptographique.

Le fournisseur de sécurité s'engage à prendre toutes les mesures utiles décrites dans l'annexe

sécurité pour assurer lors de l'exécution de la convention, la protection des informations qui peuvent être détenues ou échangées par les parties, notamment au travers :

– de la conduite d'une démarche de prise en compte des risques, validée par une décision d'homologation de sécurité du téléservice concerné ;

– de la sécurisation des développements, prenant en compte les spécificités du protocole utilisé, ainsi que de l'environnement technique du téléservice ;

– de la mise en œuvre des systèmes de détection d'événements de sécurité

Des vérifications pourront être réalisées à tout moment par les autorités de contrôle compétentes sur les services fournis (ANSSI, DINSIC ou entités mandataires) pour s'assurer de la mise en œuvre des engagements pris par le fournisseur de services en matière de sécurité des systèmes d'information. Ces vérifications incluent la possibilité de mener des audits de sécurité sur le téléservice.

En cas de manquement aux engagements de sécurité pris en application de la présente convention, la transmission des données de la DGFiP via FranceConnect pourra être coupée sur décision de la DGFiP ou de la DINSIC.

Le fournisseur de service s'engage à produire à la DGFiP et à la DINSIC :

– une copie de l'attestation d'homologation de sécurité du service concerné, signée par l'autorité d'homologation désignée par le FS.

Cette attestation doit a minima contenir les informations suivantes :

– identité de l'autorité signataire ;

– fonction et nom du signataire ;

– date de l'homologation ;

– durée de l'homologation.

Ces documents seront déposés sur l'interface mise à disposition par la DINSIC aux fournisseurs de service.

Le fournisseur de service s'engage également à mettre à jour ces documents tout au long de la vie du projet et de les fournir à la DGFiP et à la DINSIC.

Article7. Volumétrie du téléservice « $NomDuTeleservice »

Le présent téléservice peut concerner $VolumeAnnuel dossiers par an, avec un pic de charge estimé à $PicHoraire demandes par heure.

Article 8. Coût du service

Aucune contrepartie financière n'est demandée par l'une ou l'autre des parties dans le cadre de la présente convention.

Article 9. Modification de la convention et modalités de résiliation

Toute modification des dispositions de la présente convention devra faire l'objet d'un avenant signé par les parties.

Toute modification des dispositions des annexes de la convention devra faire l'objet d'une

information auprès de la partie concernée avant que la modification ne soit effectuée.

Par ailleurs, excepté pour les motifs évoqués dans l'article 3 de la présente convention, si l’une des parties souhaite résilier cette convention, elle doit en informer 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'usage du téléservice est maintenu conformément aux conditions de cette convention.

« La présente convention est établie en trois (3) exemplaires originaux dont chacune des parties conserve un exemplaire.

Fait en trois exemplaires originaux »

Fait à Paris, le , »

Pour la DINSIC
Le Directeur interministériel du numérique et du système d'information et de communication de l'État M. Henri VERDIER

Pour la DGFiP
$TitreDuRepresentantDGFIPS $RepresentantDGFiP

Pour le $NomDuFS
$TitreDuRepresentantDuFS $RepresentantDuFS

VERSION DE TRAVAIL

ANNEXE 1

Description des données transmises par la DGFiP

Lorsque l'usager effectue sa démarche administrative sur le site du fournisseur de service, il autorise ce dernier à récupérer les données fiscales nécessaires au service numérique offert par lui. FranceConnect transmet à la DGFiP l'identité pivot de l'usager. La DGFiP vérifie que cette identité pivot est identique à celle envoyée lors de la connexion à FranceConnect.

La DGFiP contrôle le certificat de chaque fournisseur de service par l'intermédiaire de l'URL d'appel utilisée par ce dernier, et s'assure de la présence d'une convention entre la DGFiP et le fournisseur de services. Si aucune convention n'existe, le traitement s'arrête.

La DGFiP procède à des contrôles visant à limiter l'accès aux seules offres de services autorisées à ce fournisseur de services dans les conditions précisées dans la présente convention. Si celui-ci n'est pas autorisé, aucune donnée n'est transmise.

Une fois les vérifications terminées, la DGFiP envoie les informations demandées uniquement au fournisseur de service. Aucune donnée fiscale n'est envoyée à FranceConnect.

Ces informations sont stockées dans un silo sécurisé du fournisseur de services.

Données échangées :

$ListeDesOSDuFS

Année de revenus mis à disposition par la DGFiP :

$ListeAnnRevFS

Affichage des données sur la page de consentement :
Les données transmises par la DGFiP devront être affichées sur la page de consentement sous la forme littérale suivante (avec l'ajout de l'origine de la donnée) :

$ListeIntituleScopeFS

VERSION DE TRAVAIL

ANNEXE 2
Qualité de service

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

- FranceConnect et API « Impôt Particulier » : disponible 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.
- Offre de couverture de service du téléservice : $OuvertureTeleserviceFS
- Taux de disponibilité : 99,9 % pour la DINSIC,

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'astreinte 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 %.

VERSION DE TRAVAIL

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONTRAT DE SERVICE TECHNIQUE

ENTRE

LE FOURNISSEUR DE SERVICE

ET

LE FOURNISSEUR DE DONNÉES DGFiP

MINISTÈRE DES FINANCES
ET DES COMPTES PUBLICS

Table des matières

1.Introduction....3
2.Contacts....4
3.Principes généraux....5
3.1.Interconnexion en production....5
3.2.Accès à notre plate-forme d'intégration DGFiP....5
3.3.Format des URL d'appel....5
3.4.Transmission du jeton d'accès....5
3.5.Contrôles d'accès aux offres de services....5
3.6.Codes retour HTTP....6
3.7.Codes revenus....6
4.Données techniques des plates-formes....7
4.1.Plates-formes DGFiP....7
4.2.Plates-formes fournisseur de service (à compléter par le FS)....7
4.3.Client_ID FranceConnect (à compléter par le FS)....7
5.API «impôt particulier »....8
5.1.OS 1: RFR et nombre de parts....8
5.1.1.URL d'appel....8
5.1.2.Scopes....8
5.1.3.Retour....8
5.2.OS2 : Adresse fiscale de taxation à l'IR (AFT)....9
5.2.1.URL d'appel....9
5.2.2.Scopes....9
5.2.3.Retour....9
5.3.OS3 : Revenus non salariaux....10
5.3.1.URL d'appel....10
5.3.2.Scopes....10
5.3.3.Retour....10
5.4.OS4 : Situation de famille....12
5.4.1.URL d'appel....12
5.4.2.Scopes....12
5.4.3.Retour....12
5.5.OS5 : Montant des pensions alimentaires perçues....14
5.5.1.URL d'appel....14
5.5.2.Scopes....14
5.5.3.Retour....14
5.6.OS6 : Existence d'un déficit sur l'année de revenus....15
5.6.1.URL d'appel....15
5.6.2.Scopes....15
5.6.3.Retour....15
5.7.OS7 : Données TH....16
5.7.1.URL d'appel....16
5.7.2.Scopes....16
5.7.3.Retour....16
5.7.4.Exceptions....16
5.8.OS8 : Revenu Brut Global....17
5.8.1.URL d'appel....17
5.8.2.Scopes....17
5.8.3.Retour....17
5.9.OS9 : Revenus Mondiaux....18
5.9.1.URL d'appel....18
5.9.2.Scopes....18
5.9.3.Retour....18

1. Introduction

Ce document a pour but de décrire les principes généraux d'interconnexion entre le fournisseur de service et le fournisseur de données DGFiP ainsi que les données techniques nécessaires à la mise en œuvre des échanges(URL d'accès, adresses IP, code erreurs...) s'appuyant sur le dispositif FranceConnect.

En préalable à la mise en œuvre du présent contrat de service technique, le fournisseur de service doit conclure une convention de service avec la DGFiP qui définit notamment les offres de services que le fournisseur de service est habilité à solliciter.

2. Contacts

Entité ou organisation	Fonction	coordonnées
DGFiP, bureau SI-1G équipe GOTHA	MOE projet FranceConnect, DLN1X	BALF : bureau.si1g-annuaire-dgfip@dgfip.finances.gouv.fr
DGFiP, bureau Cap PART	MOA projet FranceConnect, DLN1X	BALF : bureau.cappart-fc-dln1x@dgfip.finances.gouv.fr

3. Principes généraux

3.1. Interconnexion en production

Il existe trois pré-requis à la réalisation de la liaison entre un fournisseur de service et le fournisseur de données DGFiP :

- le fournisseur de service doit disposer d'un certificat client valide RGS V2.0.
- le fournisseur de service doit communiquer la ou les adresses IP sortante(s) de ses serveurs à la DGFiP
- la DGFiP doit disposer du client_id FranceConnect du fournisseur de service

3.2. Format des URL d'appel

Les URL d'appel aux offres de services mises à disposition par la DGFiP en production, sont de la forme :

`https://cft.impots.gouv.fr/API/osX/{{ANNEE}}`

API fait référence à l'API regroupant un ensemble d'offres de services.
OSX fait référence à l'offre de services appelée(Liste des OS par API à partir du paragraphe 5).

Le paramètre **ANNEE** est attendue sur 4 chiffres.

3.3. Transmission du jeton d'accès

Le jeton d'accès (accessToken) émis auprès de FranceConnect pour la récupération de données devra être transmis dans l'en-tête "Authorization" sous la forme : "Bearer: accessToken"

3.4. Contrôles d'accès aux offres de services

Outres les contrôles sur l'identité pivot du demandeur, sur la base de la convention de service conclue par le fournisseur de service, la DGFiP procède à chaque appel à des contrôles visant à limiter l'accès aux seules OS autorisées à ce fournisseur de service et dans les conditions précisées dans la convention (scopes, année de restitution, par exemple).

3.5. Codes retour HTTP

Les codes retour HTTP sont communs à toutes les offres de service DGFiP.

Code HTTP	Description
200	Transaction OK
403	Vous n'avez pas le droit d'accéder à la ressource. (exemple : scopes non valables)
404	Erreur fonctionnelle : la DGFiP ne retournera pas d'informations liées à l'identité pivot. (exemple : usager suspendu dans l'annuaire d'authentification d'impots.gouv.fr)
500	Erreur technique : Une erreur est survenue dans le parcours applicatif de la DGFiP. (exemple : panne réseau)

3.6. Codes revenus

Certaines offres de services peuvent retourner des codes revenus sur 3 caractères (ex : 1AT).
La liste des codes revenus peut varier d'une année sur l'autre.
Les codes revenus possibles ne sont pas listés dans ce document.

4. Données techniques des plates-formes

4.1. Plate-forme DGFiP

Plate-forme de production

URL	URI
https://cft.impots.gouv.fr	/impotparticulier/osX/{{ANNEE}}

4.2. Plates-formes fournisseur de service

Adresse(s) IP sortante(s)
$IP1
$IP2

4.3. Client_ID FranceConnect

Le client_ID est fourni par FranceConnect lors de la création des identifiants.

Environnement	Client_ID
Production	

5. API «impôt particulier »

5.1. OS 1: RFR et nombre de parts

5.1.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os1/{{ANNEE}}
```

5.1.2. Scopes

```
"dgfip_rfr"
"dgfip_nbpart"
```

5.1.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "rfr": 0,
      "nbPart": 1.0
}
```

Champs	Amplitude de la réponse et libellé
`rfr`	Nombre entier de 10 caractères numériques ou la valeur null. Il s'agit du revenu fiscal de référence du foyer auquel l'identité pivot a été rattachée.
`nbPart`	Nombre décimal. C'est le nombre de part du foyer fiscal.

5.2. OS2 : Adresse fiscale de taxation à l'IR (AFT)

5.2.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os2/{{ANNEE}}
```

5.2.2. Scopes

```
"dgfip_aft"
```

5.2.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "aft": "5 rue cinq appartement5 Paris 75005 paris cinq",
      "aftDetail": {
            "complementAdresse": "appartement5",
            "voie": "5 rue cinq",
            "codePostal": "75005 paris cinq",
            "commune": "Paris"
      }
}
```

Champs	Amplitude de la réponse et libellé
`aft`	Une chaîne d'une longueur de 132 caractères maximum composée de : – n° voie et libellé de la voie (37 caractères max) – complément d'adresse (30 caractères max) – libellé de la commune (30 caractères max) – code postal + nom de la localité de destination (32 caractères max) – Espaces de séparation entre les données (3 caractères max)
`aftDetail.complementAdresse`	complément d'adresse (32 caractères max)
`aftDetail.voie`	n° voie et libellé de la voie (37 caractères max)
`aftDetail.codePostal`	code postal + nom de la localité de destination (32 caractères max)
`aftDetail.commune`	libellé de la commune

5.3. OS3 : Revenus non salariaux

5.3.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os3/{{ANNEE}}
```

5.3.2. Scopes

```
"dgfip_rns"
```

5.3.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "rev": {
            "rcm": [
                  { "code": string, "valeur": string },
                  …
            ],
            "pv": [
                  { "code": string, "valeur": string },
                  …
            ],
            "fonc": [
                  { "code": string, "valeur": string },
                  …
            ],
            "pro": [
                  { "code": string, "valeur": string },
                  …
            ],
            "alpha": [
                  { "code": string, "valeur": string },
                  …
            ],
            "tspr": [
                  { "code": string, "valeur": string },
                  …
            ]
      }
}
```

Les codes de cette OS sont tous sur 3 caractères et sont décrits dans le tableau ci-après.
Les montants correspondant à ces codes sont sur 12 caractères maximum.

Seuls les codes pour lesquels il existe des éléments valorisés dans la déclaration sont donnés.
Si une catégorie de revenus ne contient pas d'éléments elle ne sera pas restituée.
Il est donc possible d'obtenir un JSON contenant, par exemple, uniquement : `{ "rev": { } }`

champs	Liste des codes
`rev.rcm`	Revenus des valeurs et capitaux mobiliers Revenus des valeurs et capitaux mobiliers exceptionnels

rev.pv	Plus-values et gains divers Revenus exceptionnels.
rev.fonc	Revenus fonciers Revenus fonciers exceptionnels
rev.pro	Revenus agricoles Revenus industriels et commerciaux professionnels Revenus industriels et commerciaux non professionnels Revenus des locations meublées non professionnelles Revenus non commerciaux professionnels Revenus non commerciaux non professionnels Produits taxables à 16 % Plus-values de cessions taxables à 16 % et moins-values à long terme
rev.alpha.code	Code Revenus commençant par une lettre.
rev.alpha.valeur	Valeur/Montant saisi dans la déclaration correspondant au code ci-avant.
rev.tspr.code	Traitements, salaires, pensions et retraites en capital taxable à 7,5 %.
rev.tspr.valeur	Valeur/Montant saisi dans la déclaration correspondant au code ci-avant.

5.4. OS4 : Situation de famille

5.4.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os4/{{ANNEE}}
```

5.4.2. Scopes

```
"dgfip_sitfam"
"dgfip_pac"
"dgfip_decl"
"dgfip_pariso"
```

5.4.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "sitFam": "string",
      "pac": {
            "nbPac": number,
            "nbPacF": number,
            "nbPacH": number,
            "nbPacR": number,
            "nbPacJ": number,
            "nbPacN": number,
            "nbPacP": number
      },
      "nmNaiDec1": "string",
      "nmUsaDec1": "string",
      "prnmDec1": "string",
      "nmNaiDec2": "string",
      "nmUsaDec2": "string",
      "prnmDec2": "string",
      "sitParIso": "string"
}
```

Champs	Amplitude de la réponse et libellé
`sitFam`	Correspond à la situation de famille. Il s'agit de la chaîne «null» ou d'un caractère qui peut prendre les valeurs suivantes : M : Marié(e) C : Célibataire D : Divorcé V : Veuf(ve) O : Pacsé(e)
`pac.nbPac`	Correspond au nombre de personnes à charge présentes dans le foyer. Il s'agit d'un nombre entre 0 et 99. Le nombre de personnes à charge correspond à la somme des : - enfants à charge (F) - enfants à charge en garde alternée (H), - personnes invalides à charge (R),

	- enfants majeurs célibataires (J), - enfants majeurs mariés ou chargés de famille (N), - petits enfants en garde alternés (P)
pac.nbPacF	Entier (2 caractères) Nombre d'enfants mineurs à charges exclusifs.
pac.nbPacH	Entier (2 caractères) Nombre d'enfants mineurs en résidence alternée.
pac.nbPacR	Entier (2 caractères) Nombre de personnes à charges invalides
pac.nbPacJ	Entier (2 caractères) Nombre d'enfants majeurs à charge célibataires
pac.nbPacN	Entier (2 caractères) Nombre d'enfants majeurs mariés/pacsés avec ou sans charge de famille et d'enfants non mariés/pacsés chargés de famille
pac.nbPacP	Entier Nombre de petits-enfants en résidence alternée
nmNaiDec1	Chaîne de caractère (60 max) ou « null » Nom de naissance déclarant 1
nmUsaDec1	Chaîne de caractère (60 max) ou « null » Nom d'usage déclarant 1
prnmDec1	Chaîne de caractère (60 max) ou « null » Prénom déclarant 1
nmNaiDec2	Chaîne de caractère (60 max) ou « null » Nom de naissance déclarant 2
nmUsaDec2	Chaîne de caractère (60 max) ou « null » Nom d'usage déclarant 2
prnmDec2	Chaîne de caractère (60 max) ou « null » Prénom déclarant 2
sitParIso	Un caractère X, T ou « null » Situation parent isolé

5.5. OS5 : Montant des pensions alimentaires perçues

5.5.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os5/{{ANNEE}}
```

5.5.2. Scopes

```
"dgfip_pensalper"
```

5.5.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "pensAlPer": integer
}
```

Champs	Amplitude de la réponse et libellé
`pensAlPer`	Un nombre entier jusqu'à 8 caractères. Montant des pensions alimentaires perçues => agrégat.

5.6. OS6 : Existence d'un déficit sur l'année de revenus

5.6.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os6/{{ANNEE}}
```

5.6.2. Scopes

```
"dgfip_inddeficit"
```

5.6.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "indDeficit": integer
}
```

Champs	Amplitude de la réponse et libellé
`indDeficit`	Nombre entier de valeur 1 ou 0. Indicateur de présence de déficit ou non imputable sur l'année

5.7. OS7 : Données TH

5.7.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os7/{{ANNEE}}
```

5.7.2. Scopes

```
"dgfip_locaux_th"
```

5.7.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "regimeTax": "string",
      "locaux": [
            {
                  "natureLocal": "string",
                  "affectation": "string",
                  "invariant": "string"
            },
            …
      ]
}
```

Champs	Amplitude de la réponse et libellé
`regimeTax`	Régime de taxation (code sur un caractère) P = principal, S = secondaire, E=dépendance L'OS ne retournera que les régimes de taxation « P » (Principale).
`locaux.natureLocal`	Type du bien (code sur 2 caractères) Ex : MA, ME, MP, AP
`locaux.affectation`	Type d'affectation du local (code sur une lettre) L'OS ne retournera que les locaux avec une affectation « H » (Habitation).
`locaux.invariant`	Identifiant du local

5.7.4. Exceptions

Si l'usager possède plusieurs TH principales, aucune donnée ne sera restituée.
Un code de retour 404 sera alors reçu par le client.

Si l'usager ne possède pas de TH principale, une erreur 404 sera également rencontrée.

5.8. OS8 : Revenu Brut Global

5.8.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os8/{{ANNEE}}
```

5.8.2. Scopes

```
"dgfip_rbg"
```

5.8.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "revenuBrutGlobal": integer
}
```

Champs	Amplitude de la réponse et libellé
`revenuBrutGlobal`	Montant du revenu brut global. Nombre entier ou « null ».

5.9. OS9 : Revenus Mondiaux

5.9.1. URL d'appel

```
https://cft.impots.gouv.fr/impotparticulier/os9/{{ANNEE}}
```

5.9.2. Scopes

```
"dgfip_rev_monde"
```

5.9.3. Retour

Au format JSON, la réponse est de la forme suivante :

```
{
      "rev": {
            "div": [
                  { "code": string, "valeur": string }
            ]
      }
}
```

Seul le code correspondant aux revenus mondiaux sera retourné par cette OS s'il est valorisé dans la déclaration de revenus.
S'il n'est pas valorisé, la catégorie « div » sera omise et le JSON retourné sera : `{ "rev": { } }`

Champs	Amplitude de la réponse et libellé
`rev.div.code`	Code revenus de catégorie 8.
`rec.div.valeur`	Valeur/Montant saisi dans la déclaration correspondant au code ci-avant.

VERSION DE TRAVAIL

ANNEXE 4

PROTOCOLE D'ECHANGES EN PRODUCTION ENTRE FRANCECONNECT ET LA DGFiP (FOURNISSEUR DE DONNEES)

I. Objet

Le présent document a pour objet de spécifier les modalités opérationnelles de la collaboration entre les services en production pour établir des échanges de données entre les Fournisseurs de Services (FS) proposés par FranceConnect, opéré par la DINSIC, et le Fournisseur de données mis à disposition par la DGFiP. L'objectif visé par les parties à travers ce partenariat est la simplification de la relation entre l'administration et ses usagers, et l'objectif du protocole est d'assurer le meilleur service possible à l'utilisateur.

1.1 Les Parties

Le présent partenariat est établi entre d'une part les responsables de la production de la Direction générale des finances publiques (DGFiP) et d'autre part, leurs homologues de la Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'Etat (DINSIC).

1.2 Objet du document

Le projet FranceConnect (FC) a l'ambition de simplifier la relation des usagers avec l'administration. Il propose à l'usager des fournisseurs de services en ligne en s'appuyant d'une part sur des fournisseurs d'identité, et d'autre part des fournisseurs de données, la DGFiP pouvant jouer les deux rôles.
Après authentification par le fournisseur d'identité, par exemple FranceConnect – Fournisseur d'identité (FI) de la DGFiP, le fournisseur de services choisi demandera à un fournisseur de données les informations nécessaires à l'accomplissement de la démarche. FranceConnect permet également le suivi par l'usager des échanges de données le concernant et garantit la confidentialité des informations.

Ce protocole porte plus spécifiquement sur le rôle de Fournisseur de Données (FD) de la DGFiP. Il détermine les conditions et modalités du partenariat concernant :

- les modalités d'informations croisées sur la gestion des mises en production,
- la gestion des incidents.

II. Gestion des mises en production

2.1 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 contacts nécessaires figurent en annexe A. Les deux parties s'engagent à ne pas communiquer ces points de contact aux usagers.

2.2 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).

Cet 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 susceptibles 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 DINSIC .

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

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

2.3 Suivi des mises en production du FC seul

Lors de toute évolution FC, en l'absence d'outil dédié à la DINSIC 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 (annexe A).

2.4 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 (cf. supra 2.2) et SWITCH (cf. infra 3.2), renforcée par courriel si nécessaire.

La DINSIC assurera la communication autour de la MEP par courriel sur la base des contacts de la liste fournie en annexe A.

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.

III. Gestion des incidents

3.1 Modalité 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 en annexe A.

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 annexe B).

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**.**

3.2 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 DINSIC. 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 œuvre 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.

3.3 Suivi des incidents du FC seul

Du fait de l'absence d'outil dédié à la DINSIC, le partage de l'information implique nécessairement une communication écrite par courriel auprès des contacts recensés en annexe A.

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.

3.4 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 DINSIC assurera la communication autour de l'incident par courriel. Les échanges se feront sur la base des contacts de la liste fournie en annexe A.

ANNEXE A – Contacts dans le cadre de la gestion des incidents

Contacts fonctionnels :

La DINSIC met à disposition de 9h 00 à 18h 00 sauf week-ends et jours fériés l'adresse électronique :

support@dev-franceconnect.fr

Les messages SWITCH seront adressés à la DINSIC à l'adresse :

support@dev-franceconnect.fr

Contacts d'urgence (premier niveau) DGFiP prioritaires en cas d'incident :

BALF fonctionnelle : bureau.si2a-dme@dgfip.finances.gouv.fr

Le fournisseur de service met à disposition de 9h00 à 18h00 sauf week-ends, jours fériés et jours de fermeture l'adresse électronique :

$CourrielContact1

$CourrielContact2

Eric REBOUILLET PETIOT (PRODUCTION)			
Tél	+ 33 1 57 33 74 09		
Mobile			
Email	eric.rebouillet-petiot@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Philippe PAQUET (SECURITE)			
Tél	+ 33 1 57 33 61 26		
Mobile			
Email	philippe.paquet@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	

Jean-Marie ULMANN (SECURITE)			
Tél	+ 33 1 57 33 72 05		
Mobile			
Email	jean-marie.ulmann@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	
	HNO	Yes	

Interlocuteurs :

Contacts FranceConnect

Laurent VOILLOT (contact pour sujets liés à la sécurité)			
Tél	+33 1 40 15 72 78		
Mobile	+33 6 48 83 90 38		
Email	laurent.voillot@modernisation.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	Yes	Yes

Eric HEIJLIGERS			
Tél	+33 1 40 15 72 79		
Mobile	+33 6 09 75 59 62		
Email	eric.heijligers@modernisation.gouv.fr	Incident	Maintenance
Disponibilité	HO	NO	Yes
	HNO	NO	NO

Contacts DGFiP

Frédérique RIEHL (MOA CAP PARTICULIERS)			
Tél	+33 1 57 33 75 67		
Mobile			
Email	frederique.riehl@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Jean-Marc SEIGNEZ (MOA CAP PARTICULIERS)			
Tél	+33 1 57 33 73 09		
Mobile			
Email	Jean-marc.seignez@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

John-James ALIX (MOA CAP PARTICULIERS)			
Tél	+33 1 57 33 63 07		
Mobile			
Email	John-james.alix@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

François WATTEZ (MOE SI1G)			
Tél	+33 1 57 33 53 45		
Mobile			
Email	françois.wattez@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Fabrice GUENIN (MOE SI1G)			
Tél	+33 1 57 33 69 57		
Mobile			
Email	fabrice.guenin@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Laurent LEPREVOST (MOE SI1G)			
Tél	+33 1 57 33 60 23		
Mobile			
Email	laurent.leprevost@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Christine LE BOURHIS (INTEX)			
Tél	+33 1 60 37 92 94		
Mobile			
Email	christine.le-bourhis@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Hugues BERNARD (MOE SI1E)			
Tél	+33 1 57 33 68 74		
Mobile	+33 6 62 12 95 81		
Email	hugues.bernard@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Eric BOULANGER (INTEX)			
Tél	+ 33 1 60 37 91 30		
Mobile			
Email	eric.boulanger@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Laurent FRAISSE (PRODUCTION)			
Tél	+33 1 57 33 74 12		
Mobile			
Email	laurent-l.fraisse@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Eric REBOUILLET PETIOT (PRODUCTION)			
Tél	+33 1 57 33 74 09		
Mobile			
Email	eric.rebouillet-petiot@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Romuald BEAUROY-EUSTACHE (PRODUCTION)			
Tél	+33 1 57 33 60 37		
Mobile			
Email	romuald.beauroy-eustache@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Jean-François LULL (PRODUCTION)			
Tél	+33 1 57 33 63 36		
Mobile			
Email	dme-lull.consultant@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

Housni AZZOUSI IDRISSI (PRODUCTION)			
Tél	+33 1 57 33 63 32		
Mobile			
Email	housni.azzouzi-idrissi@dgfip.finances.gouv.fr	Incident	Maintenance
Disponibilité	HO	Yes	Yes
	HNO	NO	NO

ANNEXE B – 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
DISPONIBILITÉ	**D1**	**D2**	**D 3**	**D4**
	Interruption acceptable au-delà de 5 jours. Pas de remise en cause des services essentiels du SI. Interruption =] 5 jours ; 15 jours]	La fonction ou le service ne doivent pas être interrompus plus de 5 jours. Les conséquences sur les services essentiels du SI sont importantes. Interruption =] 48 heures ; 5 jours]	La fonction ou le service ne doivent pas être interrompus plus de 48 heures. Les conséquences sur les services essentiels du SI sont graves. Interruption =] 4 heures ; 48 heures]	Le service doit toujours être fourni. Haute disponibilité requise. [0 ; 4 heures]
INTÉGRITÉ	**I 1**	**I 2**	**I 3**	**I 4**
	Atteinte à l'intégrité des fonctions ou informations manipulées, acceptée si détectée et signalée.	Atteinte à l'intégrité des fonctions ou informations manipulées, tolérée si détectée, signalée et corrigée dans un délai raisonnable.	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.	Atteinte à l'intégrité des fonctions ou informations manipulées inacceptable. Les fonctions et informations doivent être toujours intègres.
CONFIDENTIALITÉ	**C 1**	**C 2**	**C 3**	**C 4**
	Informations pouvant être communiquées à tout public.	Informations nécessitant une diffusion restreinte aux acteurs de la DGFIP.	Informations accessibles uniquement à des populations identifiées, authentifiées et habilitées.	Informations accessibles uniquement à des personnes habilitées et authentifiées de manière forte au travers de dispositifs de sécurité renforcés.
PREUVE ET CONTRÔLE	**P 1**	**P 2**	**P 3**	**P 4**
	Éléments de preuve non nécessaires.	Éléments de preuve nécessaires avec mise à disposition dans un délai raisonnable. Exploitation de logs « techniques » traduisant un niveau de trace « simple ».	Éléments de preuve nécessaires avec mise à disposition rapide. Exploitation de traces dites « fonctionnelles » ou « métier » traduisant un niveau de trace « détaillée ».	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**	**A 2**	**A 3**	**A 4**
	Aucune donnée nominative identifiée.	Traitement de données nominatives internes à la DGFiP : pas d'exploitation à des fins métier autres que celles prévues initialement.	Traitement de données nominatives externes à la DGFiP : pas d'exploitation à des fins métier autres que celles prévues initialement.	Besoin d'anonymat avéré : interdiction d'utiliser et d'exploiter des données directement ou indirectement nominatives.

VERSION DE TRAVAIL

Annexe 5. Sécurité du téléservice

Afin de sécuriser le téléservice qu'il propose aux usagers et assurer la protection des informations échangées avec le fournisseur de données, le fournisseur de service s'engage à mettre en œuvre les dispositions présentées ci-après.

1. Organisation SSI

Le fournisseur de service veille à mettre en place une organisation dédiée à la sécurité des systèmes d'information.

Cette organisation définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes ainsi que les modalités d'application des mesures de protection.

Dans ce cadre, le fournisseur de service s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI).

Le fournisseur de service établit une politique de sécurité des systèmes d'information (PSSI).

Les informations relatives à l'organisation SSI, notamment celles nécessaires à l'établissement des canaux de communication avec le fournisseur de données doivent être transmises à la DGFiP et à la DINSIC, préalablement à l'ouverture du service.

En cas de gestion déléguée, le fournisseur de services devra fournir les contacts de délégation.

2. Homologation de sécurité

Dans le cadre du RGS (Référentiel Général de Sécurité), le fournisseur de services veillera à procéder à l'homologation de sécurité de son téléservice (ordonnance n°2005-1516 du 8 décembre 2005, décret n°2010-112 du 2 février 2010).

L'homologation de sécurité du téléservice devra avoir été réalisée avant l'ouverture du flux de données avec la DGFiP.

L'homologation du téléservice, formalisée par une attestation d'homologation de sécurité, doit s'appuyer sur le dossier de sécurité du projet.

Si le service est délégué à un prestataire, celui-ci est tenu de fournir l'ensemble des éléments demandés dans ce document.

Le dossier de sécurité comprend a minima une analyse de risques et le plan d'actions en découlant ainsi que la politique de sécurité appliquée. Parmi les scénarii de risque envisagés, doivent être inclus ceux concernant une compromission de l'intégrité ou de la confidentialité sur les données issues du fournisseur de données DGFiP.

Le fournisseur de service s'engage à couvrir les risques portant sur le téléservice concerné et à mettre en œuvre un suivi des risques résiduels.

Le cas échéant, le dossier de sécurité comporte également les rapports d'audits de sécurité (audits statiques / dynamiques) réalisés. Le dossier de sécurité sera fourni aux chaînes de sécurité de la

DINSIC et de la DGFiP, ou à des entités mandataires (notamment l'ANSSI), sur demande de leur part.

Dans le cas où le fournisseur de service passe par un éditeur, il peut déléguer à cet éditeur l'obligation de réalisation des audits de sécurité. Néanmoins la vérification du respect de cette obligation par l'éditeur ressort de la responsabilité du fournisseur de service.

Les exigences suivantes devront être respectées pour les audits de sécurité :

- d'un point de vue méthodologique, ils doivent prendre en compte les spécifications du protocole OpenID Connect. En particulier, les tests d'intrusion réalisés dans ce cadre intégreront les modèles de menaces présentés dans les RFC 6819 et 7636, ainsi que dans Open ID specs 1.0 Security Considerations : https://tools.ietf.org/html/rfc6819
- les vulnérabilités détectées doivent être évaluées selon le standard international CVSS[1], dans sa version 3.

En cas de prestation externalisée, le fournisseur de services s'assurera que le cahier des charges de la prestation d'audit intègre bien ces points.

Le fournisseur de service s'engage à corriger, avant raccordement avec le fournisseur de données, les vulnérabilités les plus critiques.

Le renouvellement de l'homologation doit être conforme au référentiel général de sécurité :

- la durée de validité d'une homologation de sécurité ne peut excéder 5 ans.
- L'homologation doit être renouvelée au terme de sa durée de validité, mais également en cas de changement affectant le téléservice : évolution fonctionnelle ou technique majeure, changement dans l'environnement technique, ou tout élément relatif à la sécurité du système d'information considéré, par exemple la survenance d'un incident de sécurité[2].
- Le renouvellement s'appuie sur un dossier de sécurité constitué avec les mêmes éléments que le dossier de l'homologation initiale.

En cas de dépassement de la date de validité de l'homologation, la transmission des données pourra être désactivée, à l'initiative de la DGFiP ou de la DINSIC.

3. Exigences de sécurité pour le téléservice

Les exigences de sécurité listées ci-après sont requises pour le fournisseur de service en préalable à tout échange de données. Le dossier de sécurité prévu au §2 confirmera la prise en compte de chacune de ces exigences :

- S'agissant des développements, respecter les spécifications de sécurité du protocole OpenID Connect dans l'implémentation des différentes briques du dispositif : http://openid.net/specs/openid-connect-core-1_0.html#Security.

1 https://fr.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

2 Voir dans le guide de l'ANSSI sur l'homologation de sécurité une liste non exhaustive de cas de renouvellement d'une homologation : https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/

- mettre en œuvre toutes les dispositions nécessaires pour assurer la confidentialité et l'intégrité des données échangées. Notamment, celles-ci seront stockées de façon sécurisée, par exemple en utilisant un algorithme de chiffrement conforme à l'état de l'art.
- Réaliser la conservation et la purge des données échangées conformément au contenu de la déclaration faite à la CNIL pour le téléservice. Le fournisseur de services se conformera à l'acte réglementaire unique RU-048 (https://www.cnil.fr/fr/declaration/ru-048-franceconnect). Les données utilisées dans le cadre du téléservice ne devront pas être conservées au-delà de la durée nécessaire au traitement.
- Mettre en œuvre un dispositif de traces techniques (logs) à même de permettre les investigations en cas d'événement de sécurité. Ces traces doivent être conservées de manière sûre, sur une durée de 3 ans.
- Mettre en œuvre de certificats avec authentification mutuelle et assurer 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).
- Installer des logiciels de protection contre les codes malveillants sur l'ensemble des serveurs d'interconnexion, des serveurs applicatifs et des postes de travail de l'entité. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins.
- Inclure, lors de la recette du système d'information considéré, des contrôles de sécurité, à réaliser avant toute mise en production. Des outils de tests pourront notamment être utilisés pour vérifier la bonne implémentation du protocole OpenID Connect[3].
- Maintenir le niveau de sécurité de son système d'information notamment en appliquant régulièrement les correctifs mis à disposition par les éditeurs logiciels. A cet effet, une veille sera réalisée par le fournisseur de services ou son éditeur (https://www.cert.ssi.gouv.fr/)

4. Gestion des incidents de sécurité

Les différentes parties s'engagent 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
- Traitement :
  - le cas échéant, activation d'une cellule de crise ;
  - restrictions temporaires d'accès ;
  - actions d'alerte (RSSI) réciproques et de communication (Cf §1 de la présente annexe).
- Investigations :
  - rassemblement et préservation de toutes les informations disponibles pour permettre les investigations, notamment obtention des journaux couvrant la période d'investigation ; à cet effet, le fournisseur de service s'engage à fournir à ses partenaires toute information utile
  - détermination du périmètre ;
  - qualification de l'incident, identification du fait générateur et analyse d'impact.
-

3 Voir, par exemple, les projets PrOfESSOS (https://github.com/RUB-NDS/PrOfESSOS) et EsPreSSO (https://www.nds.rub.de/media/nds/veroeffentlichungen/2015/10/30/OIDS-EsPReSSO.pdf).

- 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 place 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.

Tous ces éléments doivent être formalisés dans un document d'exploitation qui sera transmis à la DINSIC préalablement à l'ouverture du service.

5. Contrôles externes

Les engagements en termes de sécurité, pris par le FS aux termes de la présente convention, pourront être vérifiés par l'ANSSI, la DINSIC et la DGFiP ; le cas échéant, les livrables des audits et le suivi de ces audits doivent être fournis sur la demande de l'une de ces entités, ainsi que l'ensemble du dossier de sécurité du téléservice.

L'ANSSI et la DINSIC pourront également faire réaliser un audit de sécurité du téléservice ; à cet effet, un environnement permettant de faire des tests d'intrusion sera mis à sa disposition par le fournisseur de services ; d'autres types d'audits – audits de site, de code, des contrats de sous-traitance… – pourront être inclus dans le périmètre de l'audit de sécurité.

Par ailleurs, avant d'accepter le raccordement d'un nouveau fournisseur de services à l'API de fourniture de données, des tests d'intrusion automatisés de sécurité pourront être effectués par la DINSIC.

6. Prestataires externes

Toute prestation réalisée par tout organisme externe au fournisseur de service est encadrée par des clauses de sécurité. Ces clauses spécifient les mesures SSI que le prestataire doit respecter. Ces clauses doivent au minimum être du même niveau que celles imposées au fournisseur de service.

L'hébergement et l'exploitation informatique des données de l'Administration doivent être réalisés sur le territoire français. Les dispositions relatives à la sécurité des systèmes d'information doivent être détaillées et portées à la connaissance de l'ANSSI, de la DINSIC et de la DGFiP.

VERSION DE TRAVAIL