RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Conditions générales d'utilisation de l'API IMPRIM'FIP

(environnement de bac à sable)

Date de publication : 25/09/2023

FINANCES PUBLIQUES

Table des matières

1. Objet....4

2. Contexte et présentation du dispositif....4

2.1 Présentation du dispositif....4

2.2 Rôle des acteurs intervenant dans le dispositif d'échange de données....4

3. Conditions d'accessibilité au dispositif....5

3.1 Conditions juridiques....5

3.2 Déclaration de conformité des traitements à la réglementation relative à la protection des données à caractère personnel....6

4. Description du dispositif de transmission des données....6

5. Les engagements des parties....7

5.1 Obligations du producteur de l'API....7

5.2 Obligations du consommateur de l'API....8

5.3 Obligations du fournisseur de données....8

6. Protection des données à caractère personnel....9

6.1 Traitements de données à caractère personnel opérés dans le cadre de l'échange de données....9

6.2 Confidentialité....9

6.3 Relations vis-à-vis des personnes physiques concernées....9

6.4 Coopération....10

6.5 Sous-traitants....10

6.6 Violation de données à caractère personnel....10

6.7 Responsabilité....11

6.8 Traitements de données opérés dans le cadre de la mise à disposition de l'API....11

7. Coût du service....11

8. Sécurité....12

9. Gestion des mises en production....13

9.1 Identification des points de contact....13

9.2 Volumétrie....14

9.3 Suivi des mises en production....14

10. Les critères DICP.....14

11. Qualité du service.....15

12. Suspension, modification et évolution du service.....15

13. Durée de validité des conditions générales d'utilisation.....15

14. Modification des conditions générales d'utilisation et modalités de résiliation 16

15. Loi applicable et litiges.....16

1. Objet

Les présentes conditions générales d'utilisation ont pour objet de définir les conditions dans lesquelles les parties peuvent utiliser l'environnement de bac à sable de l'API IMPRIM'FIP de la Direction Générale des Finances Publiques (ci-après dénommé « DGFiP »).

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

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

Le raccordement à l'API nécessite de manière cumulative :

- la saisie, par le partenaire conventionné, dans le formulaire de souscription en ligne « DataPass » du site internet api.gouv.fr, des données exactes et strictement nécessaires à la réalisation de la démarche ;
- la validation, par la DGFiP, des informations précisées dans le formulaire « DataPass » ;
- l'acceptation pleine et entière, ainsi que le respect des conditions générales d'utilisation telles que décrites ci-après.

Les données saisies dans le formulaire « DataPass » validé ainsi que l'acceptation des conditions générales d'utilisation valent convention entre la DGFiP et le partenaire conventionné.

2. Contexte et présentation du dispositif

2.1 Présentation du dispositif

L'API IMPRIM'FIP permet aux entités administratives de délocaliser le traitement de leurs courriers sortants par l'envoi de fichier mono ou multi-documents. L'impression, la mise sous pli, l'affranchissement et la remise à La Poste est réalisée par les centres éditiques industriels de la DGFiP dans un délai maximum de deux jours après le dépôt du fichier.

Ce dispositif s'inscrit dans les dispositions prises lors du séminaire interministériel du 30 août 2022 qui a validé le principe d'un accroissement de la centralisation de l'expédition des courriers de tous les ministères via l'offre de service IMPRIM'FIP de la DGFiP.

Cette démarche vise à passer un maximum du volume du courrier de l'État sur le tarif "industriel" de la Poste plus avantageux permettant ainsi de générer des économies sur les coûts d'affranchissement. La solution IMPRIM'FIP permet de moderniser les processus d'envoi du courrier et les pratiques de travail associées. C'est également une démarche durable, contribuant à la décarbonation partielle et à la sobriété énergétique des activités d'envoi du courrier.

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

2.2.1 Rôle du producteur d'API et qualité du fournisseur de données

Le producteur de l'API IMPRIM'FIP visée à l'article 2.1 est la DGFiP.

La finalité de l'API étant la mise à disposition ainsi que la modification d'information — incluant les opérations de création, de modification ou de suppression — (API dite de consultation et d'écriture), la DGFiP et le partenaire conventionné sont réputés être les fournisseurs de données (FD).

2.2.2 Rôle du consommateur d'API et qualité du fournisseur de service

Le consommateur de l'API IMPRIM'FIP visée à l'article 2.1 est le partenaire conventionné. Il est réputé être le fournisseur de service (FS).

3. Conditions d'accessibilité au dispositif

La demande d'accès à l'API se réalise sur le site internet api.gouv.fr par le biais du formulaire dématérialisé « DataPass ». Elle nécessite la création d'un compte sur le site internet précité et le remplissage du formulaire de souscription en ligne. Les présentes conditions générales d'utilisation n'ont pas vocation à couvrir l'utilisation dudit site internet.

3.1 Conditions juridiques

3.1.1 Conditions générales

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

- Le consommateur de l'API sollicitant le raccordement au dispositif doit être autorisé à demander et exploiter les données échangées par API dans le cadre de l'exercice de ses missions.
- Le périmètre des informations sollicitées par le consommateur de l'API doit être strictement nécessaire à l'exercice de la mission pour laquelle il demande les données et se justifier par des dispositions législatives ou réglementaires, ou par une délibération d'une collectivité locale, le cas échéant.

À ce titre, le consommateur de l'API devra communiquer dans le cadre de la procédure de raccordement le ou les textes législatifs ou réglementaires justifiant son accès aux données. Le producteur de l'API opérera une analyse juridique systématique afin de déterminer si le partenaire conventionné est habilité à connaître ces données dans le cadre de ses missions.

En outre, le consommateur de l'API devra fournir au producteur de l'API :

- La description de sa démarche et de l'usage qui sera fait des données
- Le périmètre des informations visées par la demande
- Le ou les services destinataires de ces données

3.1.2 Conditions spécifiques à l'environnement de bac à sable

Les données que le producteur de l'API met à disposition sont des données fictives et ne rentrent pas dans le cadre des données à caractère personnel.

Le consommateur de l'API, s'il agit en tant que fournisseur de données, devra s'assurer que les données transmises à l'API sont des données fictives, expurgées de tout élément pouvant être considéré comme une donnée à caractère personnel.

L'accès de l'API en environnement de bac à sable n'est pas conditionné aux vérifications de sécurité définis dans les CGU des environnements de production. Ces éléments sont fournis pour information et dans le but de faciliter les démarches ultérieures en annexe des présentes CGU. Cependant il se doit de respecter les engagements de sécurité détaillés en section 8.

Le consommateur de l'API s'engage à réaliser une recette fonctionnelle dont il soumettra les résultats au producteur de l'API lors de la demande de raccordement à l'API en environnement de production.

Enfin, le consommateur de l'API devra communiquer, lors de la souscription à l'environnement de bac à sable le ou les textes législatifs ou réglementaires justifiant de l'accès aux données par le biais du formulaire « DataPass ».

3.2 Déclaration de conformité des traitements à la réglementation relative à la protection des données à caractère personnel

Le consommateur de l'API n'est soumis à aucune obligation déclarative concernant les données à caractère personnel dans le cadre de l'environnement de bac à sable.

Toutefois, il est porté à sa connaissance que, dans le cadre des CGU des environnements de production, il devra, en amont du raccordement, déclarer au producteur de l'API l'accomplissement des formalités en matière de protection des données à caractère personnel, en cochant la case à cet effet dans le formulaire « DataPass » lors de la souscription à l'environnement de production.

4. Description du dispositif de transmission des données

En fonction du cadre juridique et des contrats d'interfaces publiés, le consommateur de l'API peut interroger l'API à partir des paramètres suivants :

- Référence technique unique d'un fichier permettant de connaître le statut de l'envoi d'un fichier sur la plateforme. Ce dernier est généré par l'API lors de l'envoi

d'un document et est constitué du nom du fichier, d'un horodatage et d'un identifiant du demandeur.

Le producteur de l'API, procède à une série de contrôles en amont de la consultation ou de la modification des données visant à limiter l'accès aux seules données autorisées pour le consommateur de l'API concerné au regard du périmètre et des textes juridiques précisés dans sa demande de raccordement :

- la validité du certificat du consommateur de l'API (un certificat SSL authentifiant le demandeur et garantissant la sécurisation du transfert des données) ;
- l'adresse IP de l'appelant ;
- la présence et la conformité de l'identifiant technique de l'appelant ;
- l'identité du consommateur de l'API ;
- les droits du consommateur de l'API sur les données demandées ou transmises pour la période concernée.

Une fois ces contrôles effectués, les données conformes à la contractualisation entre le consommateur de l'API et le producteur de l'API pourront être restituées ou envoyées.

Les données transmises par le producteur de l'API devront être stockées dans un silo sécurisé du consommateur de l'API permettant de garantir leur intégrité.

En revanche, si les vérifications opérées par le producteur de l'API ne sont pas conformes à la contractualisation, aucune donnée ne fera l'objet d'un échange.

L'accès à l'API s'effectue via la plateforme d'API Management (ci-après dénommé APIM) qui opère la gestion des API de la DGFiP. L'APIM offre aux partenaires conventionnés des API DGFiP des environnements de test (appelés « bac à sable ») et de production pour toutes les API et sécurise les appels effectués.

Un compte d'accès à cette plateforme sera généré et les moyens d'accès seront notifiés au responsable technique mentionné dans le formulaire de souscription « DataPass ».

5. Les engagements des parties

5.1 Obligations du producteur de l'API

Au titre de producteur d'API, la DGFiP est chargée d'instruire chaque demande de raccordement à l'API pour vérifier que ladite demande est éligible au dispositif. Elle doit notamment apprécier le caractère nécessaire des données au regard des conditions prévues par le texte législatif ou réglementaire régissant la procédure en cause.

La durée de conservation des données de l'échange (identification de l'usager qui fait l'objet de la demande, identification du consommateur de l'API, données échangées…) est limitée et justifiée au regard du besoin pour lequel elles sont collectées.

Par ailleurs, le producteur de l'API s'engage à fournir aux consommateurs de l'API toute

information utile et nécessaire en cas d'événement de sécurité susceptible d'affecter notamment l'échange de données ou les données elles-mêmes et ce, dans les meilleurs délais.

5.2 Obligations du consommateur de l'API

Il incombe au consommateur de l'API de s'assurer de/du :

- respect de la réglementation relative à la protection des données à caractère personnel ;
- la validité et de la mise à jour le cas échéant, des données de contact du responsable de traitement déclarées dans le « DataPass » ;
- traitement des données échangées pour la seule et unique finalité déclarée par le biais du « DataPass » ;
- la mise à disposition en amont de l'échange de données, de l'affichage à l'usager du périmètre et de l'origine des données échangées avec le producteur de l'API sous une forme littérale pour l'informer explicitement du dispositif d'échange de données pour la démarche envisagée et de l'ensemble des informations requises par la réglementation relative à la protection des données à caractère personnel ;
- l'accès aux données échangées aux seuls agents des services compétents ou personnels habilités pour instruire les demandes des usagers. Le ou les services destinataires des données devront être expressément communiqués au producteur de l'API par le biais du « DataPass » ;
- la mise en œuvre de toutes les mesures techniques et organisationnelles nécessaires pour garantir l'intégrité, la confidentialité et la sécurité des données échangées incluant la mise en œuvre d'un dispositif de traçabilité ;
- l'absence de stockage des identifiants au-delà du temps nécessaire au traitement de la demande de l'usager, sauf cadre juridique l'y autorisant.

De plus, préalablement à la validation de son accès à l'API, le consommateur de l'API devra :

- prendre de contact avec l'équipe DGFiP : imprimfip@dgfip.finances.gouv.fr,
- respecter la charte technique et graphique IMPRIM'FIP,
- faire valider les maquettes de courrier.

Il appartient au consommateur de l'API d'informer par écrit ses partenaires en cas de délégations de service ou recours à des contrats de sous-traitance dans le cadre de la mise en place du service ou de l'application utilisant les données échangées. Cette information doit intervenir dans un délai raisonnable avant la mise en œuvre de la délégation de service ou la sous-traitance.

Le consommateur de l'API devra également fournir par écrit au producteur de l'API toute information utile et nécessaire en cas d'événement de sécurité susceptible notamment d'affecter la transmission des données ou les données elles-mêmes et ce, dans les meilleurs délais.

5.3 Obligations du fournisseur de données

Dès qu'ils agissent en tant que fournisseurs de données, tel que défini à l'article 2.2.1, la DGFiP et le partenaire conventionné s'engagent à transmettre, pour l'usager concerné, les seules données autorisées pour le cas d'usage concerné selon les modalités décrites dans la documentation fonctionnelle et technique de l'API (publiée sur le « Store » APIM de la DGFiP).

Dans le cas où le fournisseur de données traite des données à caractère personnel, il est soumis aux obligations de respect des règles définies dans la section 6.

6. Protection des données à caractère personnel

6.1 Traitements de données à caractère personnel opérés dans le cadre de l' accès aux prestations

Dans le cadre de l'accès aux services IMPRIM'FIP par le biais de l'API, la DGFiP, opère en tant que sous-traitant pour le compte du bénéficiaire, responsable de traitement.

En conformité avec l'article 28 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, le responsable de traitement et le sous-traitant s'engagent à respecter les clauses annexées aux présentes CGU, intitulées « Obligations relatives à la protection des données à caractère personnel ».

6.2 Confidentialité

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

6.3 Relations vis-à-vis des personnes physiques concernées

Il incombe au 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 au responsable de traitement d'assurer respectivement la prise en charge de l'exercice de ces droits par les personnes physiques concernées.

6.4 Traitements de données opérés dans le cadre de la mise à disposition de l'API

La DGFiP traite les données à caractère personnel collectées :

- dans le formulaire de souscription en ligne « DataPass » du site api.gouv.fr ainsi que
- dans le cadre de l'utilisation des API par les partenaires (logs et autres traces de connexion et d'utilisation, etc.) et les échanges subséquents avec le partenaire.

Ce traitement a pour finalité la mise en place et la gestion opérationnelle des échanges de données réalisées par le biais des API mis à disposition des partenaires habilités par la DGFiP. Il est mis en œuvre dans le cadre des missions d'intérêt public de la DGFiP et de ses obligations légales au titre des dispositions du Code des relations entre le public et l'administration ou d'une autre source réglementaire spécifique.

Les données collectées dans le cadre de la souscription « DataPass » sont conservées pendant 6 ans à compter de l'arrêt de la délivrance des données par voie d'API au demandeur.

Les concepteurs et administrateurs des API au sein de la DGFiP sont les seuls destinataires de ces données.

Les personnes concernées (acteurs intervenant dans le cadre de la souscription au « DataPass » : demandeur, responsable de traitement et responsable technique) peuvent accéder aux données les concernant, les rectifier, demander leur effacement ou exercer leurs droits à la limitation du traitement de leurs données en contactant l'adresse :

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

Si vous estimez, après avoir contacté la DGFiP que vos droits ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

7. Coût du service

La prestation d'envoi de courrier n'étant pas opérante en environnement de bac à sable, les dispositions de cette section ne s'appliquent pas dans ce contexte. Toutefois, elles sont reproduites ci-dessous pour la bonne information du consommateur de l'API.

Lors de la souscription à l'environnement de production, une convention financière sera conclue entre les deux parties organisant les conditions de financement de la prestation de services.
Le montant de la prestation effectuée pour le consommateur de l'API sera calculé annuellement à partir de la volumétrie des plis déposés multipliée par le coût

d'affranchissement et le coût de production du service, fixés forfaitairement dans le projet de demande de prestation.

Ce prix fera l'objet d'une révision annuelle (au 1er janvier) afin de prendre en compte la hausse du coût de l'affranchissement et éventuellement l'augmentation du coût de production.

8. Sécurité

Dans le cadre des dispositions légales et réglementaires en matière de protection du secret et des données à caractère personnel, le consommateur de l'API et le producteur de l'API s'engagent à prendre toutes les mesures utiles et nécessaires 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 OAuth2.0[1] doivent être respectées dans l'implémentation des différentes briques du dispositif ;
- l'engagement du consommateur de l'API en matière de sécurité doit s'appuyer sur une analyse de risques et des audits de sécurité réguliers prenant en compte les spécifications du protocole OAuth2.0 précité ;
- les parties doivent s'engager à couvrir les risques portant sur leurs systèmes d'information 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.

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 : notamment l'isolation ou la 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 ;

1 https://tools.ietf.org/html/rfc6749

- qualification de l'incident, identification du fait générateur et analyse d'impact.

- Traitement :
  - si nécessaire, activation d'une cellule de crise ;
  - restrictions temporaires d'accès ;
  - actions d'alerte (RSSI) réciproques et de communication.
- Après résolution de l'incident :
  - analyse de l'incident de sécurité pour détermination de la cause et corrections associées ;
  - vérification avant remise en service que l'élément malveillant a été supprimé et que les éventuelles vulnérabilités sont corrigées ;
- Éventuelles 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 des systèmes d'information (notamment la détection de comportements anormaux) incluant un système de traçabilité des accès et actions des utilisateurs y compris ceux automatisés par robot ou traitement par lots, sur les données et processus ;
- 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 (tels que les utilisateurs ou les exploitants), des circuits d'alerte, la sensibilisation de ces acteurs ;
- des tests des processus d'alerte.

9. Gestion des mises en production

9.1 Identification des points de contact

9.1.1 Contact DGFiP pour l'assistance technique et fonctionnelle

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

apimanagement.support@dgfip.finances.gouv.fr

9.1.2 Contact DGFiP pour la souscription au « DataPass »

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

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

9.1.3 Contact du fournisseur de service

Le consommateur de l'API, en tant que fournisseur de service vis-à-vis de ses usagers, précise les contacts à privilégier dans le cadre de sa demande de raccordement à l'API formulée sur le formulaire « DataPass ».

9.2 Volumétrie

Par défaut, le quota d'appels de l'API est fixé à 50 appels par minute.

9.3 Suivi des mises en production

Il n'y a pas d'outil partagé entre les partenaires sur le suivi des mises en production. 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 quatorze (14) jours ouvrés avant leur application en conditions nominales et sept (7) jours ouvrés avant leur application en conditions d'urgence.

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

10. Les critères DICP

Le bureau architecture et norme (Bureau SI1) de la DGFiP a défini une méthode d'intégration de la sécurité dans les projets (démarche ISP).

Cette démarche comporte notamment une phase de sensibilisation globale de la sécurité du projet qui permet aux acteurs métiers de mesurer la sensibilité globale du projet en termes de disponibilité, intégrité, confidentialité, preuve et contrôle (DICP).

La sensibilité du projet (SGP) sur le périmètre d'analyse est alors évaluée à l'aide des critères de sécurité fournis en annexe de ces CGU et se traduit par un unique profil DICP. Ce profil correspond à l'évaluation des niveaux de service de la sécurité qu'il requiert pour chacun de ces critères.

S'agissant du projet API IMPRIM'FIP dans la mise en œuvre par le producteur de l'API, le profil DICP est le suivant :

D	I	C	P
3 (24h)	3	3	2

11. Qualité du service

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

- API : ouverture toute l'année ;
- Périodes sensibles identifiées : Périodes d'activités du domaine professionnel ;
- Plages d'ouverture du service : 0:00-24:00, 7j/7 (service non disponible pour maintenance sur une plage de 2 heures entre 23:00 et 6:00) ;
- Offre de couverture de service de la DGFiP : 7:00-20:00 ;
- L'offre de couverture de service et le taux de disponibilité du téléservice est précisé par le consommateur de l'API lors de sa demande de raccordement à l'API.

La mesure du taux de disponibilité se fait sur la plage d'ouverture du service, que les indisponibilités soient programmées ou non.

- Pas de besoin d'astreintes les soirs et les week-ends ;
- Garantie du temps de rétablissement en cas d'incident estimé 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, modification et évolution du service

Le producteur de l'API se réserve la liberté de faire évoluer, de modifier ou de suspendre, sans préavis, le service pour des raisons de maintenance, de sécurité ou pour tout autre motif jugé nécessaire.

En pareille hypothèse, le consommateur de l'API en sera dûment averti par écrit et dans les meilleurs délais.

13. Durée de validité 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.

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

Les termes des présentes CGU peuvent être modifiées ou complétées à tout moment, sans préavis, en fonction des modifications apportées au service, de l'évolution de la législation ou pour tout autre motif jugé nécessaire.

Toute modification des CGU fera l'objet d'une information auprès de la partie impactée.

En cas de nullité d'une ou plusieurs des clauses des présentes CGU en application d'une loi, d'un règlement ou à la suite d'une décision définitive rendue par une juridiction compétente, les autres clauses des CGU conserveraient leur force obligatoire dans la limite de ladite décision.

Par ailleurs, si l'une des parties souhaite mettre fin à l'échange de données avec l'API, elle en informe l'autre partie par écrit, en indiquant les motifs de sa décision.

Un préavis de deux mois est alors nécessaire avant que la résiliation ne soit pleinement effective. Durant cette période, l'échange de données via l'API est maintenu conformément aux présentes CGU.

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

La DGFiP ne peut être tenue responsable des pertes et/ou préjudices, de quelque nature qu'ils soient, qui pourraient être causés à la suite d'un dysfonctionnement ou d'une indisponibilité du service. De telles situations n'ouvriront droit à aucune compensation financière.

Aucune des parties ne peut être tenue pour responsable de toute inexécution ou retard dans l'exécution de ses obligations par suite d'évènements échappant au contrôle raisonnable d'une partie, tels que les attaques par déni de service, la défaillance d'un hébergeur ou d'un fournisseur d'accès ou de service, les grèves, les pénuries, les émeutes, les incendies, les cas de force majeure, les catastrophes naturelles, la guerre et le terrorisme.

Les présentes CGU et tous les différends qui en découlent ou qui s'y rapportent, seront régis exclusivement par la loi française.

Les tribunaux français auront compétence exclusive pour trancher tout différent découlant des CGU, de leur interprétation ou application.

Chaque partie reconnaît la compétence exclusive de ces tribunaux et s'y soumet.

Glossaire	
APIM	API Management (plateforme de gestion des API de la DGFiP)
Bac à sable	Environnement de test (exploitant des données fictives)
CGU	Conditions générales d'utilisation
DataPass	Formulaire de souscription pour l'habilitation juridique d'accès aux données restreintes
DGFiP	Direction Générale des Finances Publiques
DTNum	Délégation à la transformation numérique
FD	Fournisseur de données (tel que défini à l'article 2.2.1)
FS	Fournisseur de services (dans le cas présent, le partenaire conventionné)
Production	Environnement de production (exploitant des données réelles)
Responsable de traitement	Personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement
RGPD	Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
RGS	Référentiel général de sécurité
RSSI	Responsable de la Sécurité des Systèmes d'Information

Annexes

Tableaux des critères DICP

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.**

Engagements de sécurité pour les environnements de production

Note : Cette section reprend les CGU de production relatives aux engagements de sécurité du consommateur de l'API lorsqu'il demande un accès sur les environnements de production. Elles sont reprises à des fins d'information du consommateur de l'API afin qu'il puisse en tenir compte et lui offrir la possibilité d'anticiper les actions nécessaires pour y répondre. De ce fait, les éléments qui sont décrits dans cette annexe n'engagent pas le consommateur de l'API vis-à-vis de l'environnement de bac à sable, objet des présentes CGU.

Engagements concernant le niveau de sécurité

Le consommateur de l'API doit attester formellement du niveau de sécurité du service qu'il opère auprès de la DGFiP.

Cela peut prendre la forme :

1. pour les autorités administratives auxquels le Référentiel général de sécurité (RGS) s'applique, d'une attestation d'homologation de sécurité ;
2. pour les consommateurs de l'API ne relevant pas du champ d'application du RGS, de la fourniture d'un questionnaire de sécurité renseigné selon le modèle fourni par la DGFiP.

Homologation de sécurité

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

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

Lorsque l'homologation de sécurité comporte des réserves, ou prend la forme d'une autorisation provisoire d'emploi, un échange est réalisé entre le consommateur de l'API et le producteur de l'API afin d'expliciter les réserves, et permettre de valider l'ouverture des échanges en production.

Le consommateur de l'API s'engage à communiquer une nouvelle attestation d'homologation de sécurité trois (3) mois avant la fin de la période de validité de l'homologation de sécurité actuelle ou de l'autorisation provisoire d'emploi si celui-ci souhaite encore bénéficier du raccordement. En l'absence d'une telle transmission, l'échange de données sera suspendu jusqu'à ce que le consommateur de l'API communique ce document au producteur de l'API.

Enfin, le consommateur de l'API s'engage à informer le producteur de l'API lorsque les évolutions de risque qu'il identifie dans son processus courant de suivi des homologations font apparaître le besoin d'une nouvelle homologation, ainsi qu'à communiquer une nouvelle attestation d'homologation dès que possible.

Questionnaire de sécurité

Dans cette procédure, le producteur de l'API transmet au consommateur de l'API un modèle de questionnaire de sécurité qu'il complète en parfaite transparence et le lui retourne dans le cadre du processus de souscription.

Ce questionnaire répond à deux groupes d'interrogations :

- un premier groupe, qui permet de prendre de manière directe une décision d'ouverture ou de refus d'ouverture des échanges en production.
- un deuxième groupe, qui fait l'objet d'une analyse approfondie par la DGFiP, et qui peut conduire celle-ci à émettre des préconisations de renforcement ou d'ajustement du dispositif opérationnel ou de sécurité du consommateur de l'API. Ce dernier s'engage par principe dès la souscription à les examiner et à planifier leur réalisation.

Dans l'hypothèse où l'analyse approfondie des réponses du consommateur de l'API ferait apparaître un risque critique pour les données de la DGFiP, une résolution sous contrainte de délai peut être demandée au consommateur de l'API, voire une décision de coupure préemptive peut être prise ; décision dont serait informé le consommateur de l'API.

De la même manière qu'une homologation a une durée limitée de validité, afin de rendre récurrent le contrôle de la cohérence entre les risques et les mesures prises, **le questionnaire de sécurité devra être mis à jour régulièrement, au plus, tous les trois ans par le consommateur de l'API, et adressé au producteur de l'API.**

Obligations relatives à la protection des données à caractère personnel

CLAUSE n°1 – DÉFINITIONS RÉGLEMENTAIRES

1.1. « Données à caractère personnel » : Toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

1.2. « Données à caractère non personnel » : Données qui ne sont pas des données à caractère personnel au sens du RGPD à savoir d'une part, les données qui, au départ, ne concernaient pas une personne physique identifiée ou identifiable et d'autre part, les données qui étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes.

1.3. « Données mixtes » : Tout ensemble de données mixte comportant à la fois des données à caractère personnel et des données à caractère non personnel.

1.4. « Traitement » : Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

1.5. « Personne publique » : Responsable de traitement consacré par la réglementation nationale et européenne relative à la protection des données à caractère personnel, c'est-à-dire la personne morale, l'autorité publique, le service qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens d'un traitement et décide d'en collecter les données personnelles.

1.6. « Responsable du traitement » : Personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou d'un État membre. En spécifiant et en utilisant les Services IMPRIM'FIP par le biais de l'API, la personne publique bénéficiaire revêt la qualité de Responsable de Traitement

1.7. « Sous-traitant » : Prestataire agréé par la personne publique bénéficiaire pour exécuter une partie des prestations dans le cadre d'un contrat de sous-traitance établi par les présentes clauses. Ce prestataire est un sous-traitant direct (de niveau 1) ou un sous-traitant indirect (de niveau 2 et de niveaux inférieurs) du titulaire. Il correspond au sous-traitant consacré par la réglementation relative à la protection des données à caractère personnel. Dans le cadre de l'accès aux services IMPRIM'FIP par le biais de l'API, la DGFiP opère en tant que sous-traitant pour le compte du bénéficiaire.

1.8. « Personne concernée » : Personne physique dont les données personnelles font l'objet d'un traitement dans le cadre des prestations prévues par les présentes clauses.

1.9. « Réglementation nationale et européenne sur la protection des données à caractère personnel » : Loi n°78-17 du 6 janvier 1978 modifiée, Règlement 2016/679/UE et Directive 2016/680/UE des 27 avril 2016 fixant les conditions d'utilisation des données à caractère personnel.

1.10. « Pseudonymisation » : Traitement qui garantit que des données à caractère personnel ne pourront plus être attribuées à une personne physique précise sans avoir recours à des informations supplémentaires conservées séparément et soumises à des mesures techniques et organisationnelles.

1.11. « Violation de données à caractère personnel » : Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées ou l'accès non autorisé à de telles données.

1.12. « Mesures techniques et organisationnelles » : Mesures destinées à protéger les données personnelles contrer une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute forme illicite de traitement.

CLAUSE n°2 – POLITIQUE DE CONFORMITÉ AU RGPD

2.1. Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

2.2. Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après dénommé le « RGPD »).

2.3. Les parties s'engagent également à respecter la réglementation en vigueur applicable au traitement de données mixtes et, en particulier, le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un

cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne applicable depuis le 18 juin 2019 et les lignes directrices de la Commission européenne du 29 mai 2019 relatives au règlement applicable au libre flux des données à caractère non personnel dans l'Union européenne.

2.4. Lorsque les échanges intervenus dans le cadre des présentes clauses sont constitués d'un ensemble composite intégrant à la fois des données à caractère personnel et des données à caractère non personnel, le niveau de protection mis en œuvre doit tenir compte des prescriptions prévues par l'article 2.2 du Règlement 2018/1807 et par l'article 2.2 des lignes directrices de la Commission européenne du 29 mai 2019. En pareille situation, les conditions et les modalités d'utilisation des données à caractère non personnel et des données à caractère personnel de l'ensemble sont respectivement définies par le Règlement (UE) 2018/1807 pour les premières et par le Règlement (UE) 2016/679 pour les secondes. Lorsque les données à caractère non personnel et les données à caractère personnel sont inextricablement liées, les droits et obligations en matière de protection des données découlant du RGPD s'appliquent pleinement à l'intégralité de l'ensemble de données mixtes, même lorsque les données à caractère personnel ne représentent qu'une petite partie de l'ensemble de données.

2.5. Les Parties s'engagent également à respecter toute évolution de la législation ou de la réglementation française ou européenne qui impacterait en ce domaine les conditions d'exécution des présentes clauses.

CLAUSE n°3 – DESCRIPTION DES TRAITEMENTS FAISANT L'OBJET DES PRESTATIONS

3.1. Le Sous-traitant et ses Sous-traitants ultérieurs sont autorisés à traiter pour le compte de la personne publique les données à caractère personnel nécessaires pour fournir les services liés à l'utilisation de l'environnement de production de l'API IMPRIM'FIP de la Direction Générale des Finances Publiques.

Les opérations réalisées sur demande de la personne publique bénéficiaire par le Sous-traitant et ses Sous-traitants ultérieurs ont vocation à conférer à ces derniers un accès aux données à caractère personnel traitées dans ce cadre.

3.2. Ces opérations sont réalisées en exécution des prestations suivantes :

– Mise à disposition des moyens de production éditiques pour impression et envoi à distance des courriers

3.3. Le traitement mis en œuvre répond aux caractéristiques suivantes :

3.3.1. Les finalités du traitement sont :

- La gestion et le suivi des courriers envoyés et reçus par le responsable de traitement ;

- Le suivi statistique.

3.3.2. Les catégories de données à caractère personnel traitées sont :

- Données d'identification :

• des utilisateurs de l'interface IMPRIM'FIP : Nom, Prénom, Adresse Mail ;

• des destinataires des courriers : Nom, prénom et adresse du destinataire.

- Autres données :

• codification des courriers ;

• toutes données contenues dans les courriers.

3.3.3. Les catégories de personnes concernées sont :

- Les utilisateurs dûment habilités à IMPRIM'FIP

- Les destinataires des courriers

3.4. La durée des opérations de traitement précitées réalisées sur les données à caractère personnel par le Sous-traitant et ses Sous-traitants ultérieur s'étend pendant toute la durée de la prestation.

CLAUSE n°4 – CONDITIONS DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

4.1. Le Sous-traitant s'engage à :

• traiter les données uniquement pour la ou les seule(s) finalité(s) qui font l'objet des présentes clauses;

• traiter les données conformément aux instructions documentées de la personne publique;

• garantir la confidentialité des données à caractère personnel traitées faisant l'objet des présentes clauses ;

• veiller à ce que les personnes autorisées à traiter les données à caractère personnel objet des présentes clauses s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

• prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ;

• édicter à son personnel des directives relatives à la mise en œuvre des mesures prévues par la réglementation nationale et européenne relative à la protection des données à caractère personnel et à la démonstration du respect de cette dernière. L'application par le Sous-traitant de codes de conduite ou de mécanisme de certification approuvés, voire d'indications données par un délégué à la protection des données peut servir à démontrer le respect des obligations incombant à la personne publique.

4.2. Lieu du traitement et transfert de données à caractère personnel

4.2.1. Le Sous-traitant garantit, pendant toute la durée des prestations, que l'intégralité des données à caractère personnel sont, en exécution de la présente convention, traitées et plus généralement rendues accessibles exclusivement au sein :

- de l'Espace économique européen ;

- ou d'un État tiers bénéficiant d'une décision d'adéquation au sens de l'article 45 du RGPD .

4.2.2. A défaut, en cas de transferts résultant de la réalisation des prestations, le Sous-traitant s'engage à mettre en oeuvre les garanties appropriées ou des règles d'entreprise contraignantes au sens des articles 46 et 47 du RGPD, le cas échéant complétées par des mesures supplémentaires visant à garantir qu'il ne pourra pas y être fait échec dans l'État tiers de destination, dans le strict respect de la jurisprudence.

4.2.3. Les garanties apportées par le sous-traitant sur ce point doivent non seulement couvrir l'hébergement des données, mais également toutes les opérations de traitement réalisées par le Sous-traitant ou par les Sous-traitants ultérieurs auxquels pourraient le cas échéant être confiées certaines opérations de traitement (telles que maintenance, assistance...).

4.2.4 Le sous-traitant doit ainsi pouvoir garantir que les données traitées ne peuvent pas être rendues accessibles à des destinataires, y compris des autorités administratives ou judiciaires, situés hors de l'Espace économique européen sans que soit respecté le droit applicable, et en particulier le RGPD. Le sous-traitant détaillera les moyens mis en place pour y répondre.

4.2.5. Préalablement à tout transfert, le Sous-traitant en informe le responsable de traitement dans un délai raisonnable.

4.3 Destruction ou renvoi des données à caractère personnel

Au terme de la prestation de services relatifs au traitement des données à caractère personnel, le Sous-traitant s'engage au choix de la personne publique qui sera spécifié par écrit le moment venu à :

- détruire toutes les données à caractère personnel ou

- à les lui renvoyer. Le renvoi doit s'accompagner de la destruction de toutes les

copies existantes dans les systèmes d'information du Sous-traitant et des Sous-traitants. Le Sous-traitant et ses Sous-traitants ultérieurs justifient par écrit de la destruction.

CLAUSE n°5 – OBLIGATIONS DU SOUS-TRAITANT À L'ÉGARD DES SOUS-TRAITANTS ULTÉRIEURS

5.1. Le Sous-traitant peut faire appel à un ou plusieurs Sous-traitants pour mener des activités de traitement spécifiques.

5.2. Le Sous-traitant s'engage à ne pas recruter un autre Sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le Sous-traitant informe préalablement et par écrit la Personne publique de tout changement envisagé concernant l'ajout ou le remplacement de Sous-traitants ultérieurs. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-traitant. Afin d'obtenir l'acceptation et l'agrément de l'acheteur, le Sous-traitant doit présenter son Sous-traitant par le biais d'un acte de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou tout autre document équivalent.

5.3. Le Sous-traitant s'engage à respecter et à faire respecter par l'ensemble des Sous-traitants directs et indirects ainsi qu'à leurs personnels respectifs les mêmes obligations en matière de protection de données à caractère personnel que celles fixées dans les présentes clauses, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Pour ce faire, le Sous-traitant s'engage à insérer et à faire insérer dans les différents contrats de sous-traitance les clauses de protection des données à caractère personnel adoptées par la Commission européenne et/ou par la CNIL.

5.4. Si les Sous-traitants ne remplissent pas leurs obligations en matière de protection des données, le Sous-traitant demeure pleinement responsable devant le responsable de traitement de l'exécution de ses obligations par ces derniers. Le Sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les prestations définies par les présentes clauses.

CLAUSE n°6 – OBLIGATIONS DE LA PERSONNE PUBLIQUE À L'ÉGARD DU SOUS-TRAITANT

La personne publique s'engage à :

- fournir au Sous-traitant les données visées à la clause n°3 des présentes ;

- documenter par écrit toute instruction concernant le traitement des données par le Sous-traitant ;

- veiller, au préalable et pendant toute la durée du traitement, au respect des

obligations prévues par le règlement européen sur la protection des données de la part du Sous-traitant.

CLAUSE n°7 – REGISTRE ET DOCUMENTATION DES TRAITEMENTS

7.1. Registre des catégories d'activités de traitement

7.1.1. Le Sous-traitant s'engage à tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la personne publique en vue d'une mise à disposition de la CNIL sur demande de celle-ci.

7.1.2. Le registre se présente sous une forme écrite y compris électronique et comprend :

- le nom et les coordonnées de la personne publique pour le compte duquel il agit, du Sous-traitant et des éventuels sous-traitants ultérieurs ;

- les noms et les coordonnées du délégué à la protection des données du Sous-traitant ;

- les catégories de traitements effectués pour le compte de la personne publique ;

- si possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel,

- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,

- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique,

- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;

- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées.

7.2. Documentation

Le Sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

CLAUSE n°8 – SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL

8.1. Le Sous-traitant exécute, sous le contrôle de la personne publique, les prestations prévues par les présentes clauses en mettant en œuvre les mesures techniques et organisationnelles appropriées et en garantissant aux données à caractère personnel un niveau de sécurité adapté aux risques, compte tenu de l'état des connaissances disponibles et des coûts induits par le traitement des données.

8.2. Les mesures mises en œuvre à ce titre privilégient notamment :

- les techniques de pseudonymisation et de chiffrement des données à caractère personnel,

- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,

- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique puis

- les mesures de sécurité prévues par ses codes de conduite, interne et/ou par toute certification si le Sous-traitant en dispose.

8.3. Il met en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données à caractère personnel.

8.4. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral. La personne publique et le Sous-traitant prennent des mesures afin de garantir que toute personne physique qui, pour l'exécution des prestations, accède à des données à caractère personnel, agit bien sous l'autorité de l'un d'entre eux.

8.5. Le Sous-traitant s'engage à utiliser et à faire utiliser par les Sous-traitants ultérieurs des moyens conformes à la politique générale de sécurité des systèmes d'information de l'État (circulaire du Premier ministre du 17 juillet 2014) et des ministères économiques et financiers (Arrêté du 1er août 2016), pour :

- garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes d'information,

- rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais adaptés en cas d'incident physique ou technique.

8.6. Conformément à la réglementation nationale et européenne relative à la protection des données à caractère personnel, le Sous-traitant s'engage à préserver et à faire préserver par les Sous-traitants ultérieurs la sécurité des informations et des données qui lui sont confiées en prenant toute mesure adaptée. Ces mesures visent à empêcher que les données à caractère personnel soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Le Sous-traitant informera son personnel et sensibilisera les Sous-traitants ultérieurs qui pourraient intervenir pour son compte sur les obligations de sécurité informatique mises à leur charge.

8.7. Prestations en environnement IPV6

8.7.1. Le Sous-traitant et les Sous-traitants ultérieurs sont informés que la réalisation des prestations dans un environnement naissant IPV6 voire dans un environnement passerelle de transition IPv4/IPv6 est de nature à réduire la sécurité informatique du patrimoine logiciel et matériel de la personne publique :

- impacts sur les données et les traitements de la DGFIP exploités pour son compte ;

- impacts sur les flux informatiques échangés avec les partenaires de la personne publique ;

- impacts sur le dimensionnement des services support (maintenance, profils métier notamment).

8.7.2. A ce titre, chaque partie prend les mesures nécessaires et les précautions utiles pour renforcer la sécurité informatique des prestations et garantir la protection des données à caractère personnel au regard :

- de la nature des données et des risques soulevés par leur traitement,

- des contraintes réglementaires imposant la prise en compte de normes techniques spécifiques.

8.8. Prestations adossées à des solutions de type cloud

Dans l'hypothèse où les prestations seraient exécutées au moyen de solutions en nuage (de type « cloud ») nécessaires à l'exercice des missions confiées, le Sous-traitant s'engage à héberger et à faire héberger les données de production mises à disposition par la personne publique en un lieu géographique relevant d'une législation qui assure un niveau de protection des données à caractère personnel au moins équivalent à celui assuré par la réglementation nationale et européenne.

En outre, si le prestataire offrant la solution en nuage est soumis à la législation d'un pays

tiers ne permettant pas d'assurer un niveau de protection approprié des données personnelles au regard du RGPD, notamment en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données, le Titulaire s'engage :

– à signer, s'il est le prestataire, ou à faire signer au sous-traitant-ultérieur prestataire, les clauses contractuelles types 2021/914 de la Commission européenne ;

– à informer la personne publique de tout recours à une solution en nuage préalablement à l'exécution des prestations correspondantes. À cette occasion le Sous-traitant communique à la personne publique les mesures techniques et organisationnelles supplémentaires qu'il s'engage à mettre en œuvre pour établir un niveau de protection suffisant, en assurant a minima la mise en place d'une procédure de chiffrement garantissant la maîtrise de la gestion des clés par le responsable de traitement afin d'empêcher la lecture des données par des tiers.

CLAUSE n°9 – DEVOIR D'INFORMATION ET DEVOIR D'ALERTE

9.1. Le Sous-traitant s'engage à signaler et à faire signaler à la personne publique dans un délai inférieur à 5 jours calendaires tous les éléments qui lui paraîtraient de nature à compromettre la bonne exécution des présentes clauses.

9.2. Sécurité informatique

9.2.1. Le Sous-traitant s'engage à informer le responsable de traitement et à être informé par ses Sous-traitants de :

- tout incident de sécurité concernant les moyens informatiques utilisés au titre des prestations (intrusion logique, altération malveillante, dégradation volontaire, infection par virus informatique, disparition de supports exploités sur les lieux d'exécution des prestations),

- tout événement affectant ou susceptible d'affecter la sécurité ou le fonctionnement des systèmes d'information d'importance vitale de la personne publique au sens des articles L. 1332-6-2 et R. 1332-41-10 du code de la défense nationale dès lors que ceux-ci sont concernés par l'exécution des prestations,

- toute évolution qui affecterait les conditions de traitement et d'exploitation des données à caractère personnel envisagées pour exécuter les prestations prévues par les présentes clauses.

9.2.2. A titre indicatif, sont concernés :

- les solutions de virtualisation de traitements lorsque les fonctionnalités mises en œuvre permettent de transférer des données entre des serveurs physiques implantés dans des pays dont l'un d'eux relève d'une réglementation qui ne garantit pas un niveau de protection des données à caractère personnel adéquat ou équivalent à celui prévu par la réglementation européenne (cas des migrations à chaud de machines

virtuelles notamment),

- les déménagements de serveurs hébergeant des traitements et des données accédées et/ou exploitées pour le compte de la personne publique,

- les moyens d'accès et de transfert de données à caractère personnel (solutions d'authentification, protocoles d'échanges de données notamment).

9.2.3. Dans tous les cas, le Sous-traitant vérifie et s'engage à faire vérifier par ses Sous-traitants que l'environnement et les conditions d'exploitation des données à caractère personnel respectent les standards et les normes de sécurité informatiques validés par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) et repris dans la politique générale de sécurité des systèmes d'information de l'État (circulaire du Premier ministre du 17 juillet 2014) et des ministères économiques et financiers (Arrêté du 1er août 2016).

9.3. Instruction contraire à la réglementation

Si le Sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données, il en informe immédiatement le responsable de traitement.

9.4. Transfert de données vers un pays tiers

9.4.1. Les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Il est rappelé que tout transfert de données à caractère personnel, au bénéfice de toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé. A défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le sous-traitant suspend tout transfert et informe le responsable de traitement en vue d'envisager, le cas échéant, l'adaptation des modalités d'exécution de la convention permettant le respect des exigences du RGPD.

9.4.2. Préalablement à tout transfert vers un pays tiers ou vers une organisation internationale situé(e) en dehors du territoire de l'Union européenne et/ou en dehors de l'Espace Économique Européen dans les cas énumérés au point 4.2, le sous-traitant en informe le responsable de traitement dans un délai raisonnable.

9.5. Tout manquement constaté à ces obligations constitue une faute du sous-traitant.

CLAUSE n°10 – NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

10.1. Notification des violations à la personne publique

10.1.1. Le Titulaire s'engage à notifier dans un délai de 48 heures à la personne publique toute violation de données à caractère personnel en rapport avec l'exécution des prestations après en avoir pris connaissance.

10.1.2. Cette notification contient au moins :

• la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

• le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

• la description des conséquences probables de la violation de données à caractère personnel

10.1.3. Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

10.2. Notification des violations aux personnes concernées

10.2.1.Le responsable de traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. Le Sous-traitant lui apporte son assistance sur cette communication à la demande du responsable de traitement et compte tenu de la nature du traitement, des informations à la disposition du Sous-traitant et des compétences du Sous-traitant.

10.2.2.La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

• la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

• le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

• la description des conséquences probables de la violation de données à caractère personnel ;

• la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y

compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

10.3. Tout manquement constaté à ces obligations constitue une faute du Sous-traitant et/ou de ses Sous-traitants.

CLAUSE n°11 – DEVOIR DE COOPÉRATION

11.1. Le Sous-traitant et la personne publique s'engagent à une coopération réciproque et loyale pour la bonne exécution des prestations et le traitement licite des données à caractère personnel qui en découle.

11.2. Désignation d'un Délégué à la Protection des Données

11.2.1. Le Sous-traitant s'engage à désigner et à faire désigner par ses Sous-traitants chacun pour ce qui les concerne un délégué à la protection des données (DPD).

11.2.2. Il en communique le nom et les coordonnées à la personne publique ainsi que toute modification afférente.

Le Sous-traitant veille à ce que le DPD soit associé en temps utile, à toutes les questions relatives à la protection des données à caractère personnel que soulèverait l'exécution des prestations.

11.3. Audits des traitements par la personne publique

11.3.1. La personne publique se réserve la possibilité de tester, analyser et évaluer régulièrement, les mesures techniques, organisationnelles et de mise en conformité des process métiers afin de vérifier leur efficacité. Ces vérifications peuvent prendre la forme d'un audit sur place ou sur pièce.

11.3.2. Le Sous-traitant s'engage à permettre la réalisation des audits décidés par la personne publique et d'y contribuer. Il s'engage à permettre le déroulement des contrôles que la CNIL pourrait effectuer sur place ou sur pièces sur les traitements de données personnelles mis en œuvre pour les prestations prévues par les présentes clauses.

11.4. Mise à disposition des informations requises par les institutions publiques

Sur demande de la personne publique, le Sous-traitant lui communique toute précision :

- garantissant à la CNIL la régularité des traitements automatisés de données personnelles utilisés ou élaborés pour les besoins de l'exécution des prestations et

- permettant de répondre aux questions parlementaires (éléments statistiques et volumétriques volumétrie de certaines catégories d'informations).

11.5. Intervention au titre des installations d'importance vitale de la personne publique

11.5.1. Sur demande de la personne publique, le Sous-traitant l'assiste dans le

cadre des procédures d'audit et de contrôle susceptibles d'être déployées dans les sites classés « points d'importance vitale » notamment.

11.5.2. Il apporte, à ce titre, et en tant que de besoin, toute information permettant à la personne publique, aux experts et aux membres de la commission de défense et de sécurité de vérifier et de constater que les mesures de protection mises en œuvre dans les installations d'importance vitale notamment, et applicables aux prestations de l'accord-cadre, ne contiennent pas de failles de sécurité évidentes.

11.6. Assistance demandée par la personne publique

Dans la limite des informations disponibles, le Sous-traitant s'engage à assister la personne publique à sa demande et à obtenir de ses sous-traitants une assistance identique dans les cas suivants :

- donner suite, dans les délais requis, aux demandes et actions exercées à son encontre par les personnes concernées au titre de la réglementation relative à la protection des données à caractère personnel,

- réaliser l'analyse d'impact relative à la protection des données et la consultation préalable de la CNIL,

- honorer son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (droits d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement.

CLAUSE n°12 – RESPONSABILITÉ

12.1. Conformément aux dispositions de l'article 82 du RGPD toute personne physique ayant subi un dommage matériel ou moral du fait d'une violation de la réglementation en matière de protection des données à caractère personnel notamment le RGPD et la LIL, a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. Il est convenu que le Responsable de traitement ou le Sous-traitant et le cas échéant ses sous-traitants ultérieurs sont tenus responsables du dommage subi par la personne physique concernée à hauteur respective de leur part de responsabilité dans celui-ci.

12.2. Le Responsable de traitement, le Sous-traitant et le cas échéant, ses sous-traitants ultérieurs sont exonérés de responsabilité s'ils prouvent que le fait qui a provoqué le dommage qu'a subi la ou les personnes physiques concernées par le traitement, ne leur est nullement imputable.